Gift card scams generate billions for fraudsters and industry—how one 83-year-old fell into the 'fear bubble'

August 24 2024, by David P. Weber and Jake Bernstein

Credit: Godisable Jacob from Pexels

Wednesday morning, the day before Thanksgiving, Mae awoke, set her hair in curlers and switched on her laptop. The screen froze and a

message appeared. It said her Safari web browser had encountered a problem, and a link offered to connect the 83-year-old to the Apple Computer Company. Mae clicked it.

She didn't know it yet, but Mae, like millions of Americans each year, had fallen into the grip of fraudsters. Over the next 10 hours, the criminals would try several methods to steal her money. The one that worked without a hitch was getting her to buy gift cards. The common cards, from retailers such as Target, Apple and Amazon, are sold on racks in drugstores and supermarkets. They're better than cash for a fraudster, more portable and just as anonymous. Once criminals have the gift card numbers, they use them to purchase goods online, at stores around the world, or sell or trade them in illicit marketplaces on the dark web, Telegram or Discord.

An estimated US$8 billion is stolen annually from seniors age 60 and older through stranger-perpetrated frauds, according to AARP. Increasingly, gift cards are a leading fraud payment method reported by older adults, according to the Federal Trade Commission.

Mae's story is one of many such cases that prompted us—a fraud and forensic accounting professor who is a former top financial regulator, and a Pulitzer Prize-winning investigative reporter—to explore how cracks in the financial regulatory system dating to the Civil War have been exploited by fraudsters and corporations.

The investigation shows that federal regulators have consistently failed to protect the public from gift card fraud and have failed to give gift cards consumer protections like those afforded to credit and debit cards. Congress, in turn, has largely deferred to these regulators. Meanwhile, efforts to rein in the industry on the state and federal level have been met with successful opposition from lobbyists and gift card trade groups. When fraud does occur, gift card retailers are often less than helpful in

assisting law enforcement in helping to track down the criminals.

One of us learned about Mae's case in his work as a fraud examiner and has seen dozens of similar cases. Mae, who lives in Maryland, is unwilling to publish her last name for fear of being revictimized, as well as sheer embarrassment, but she still wants people to know the story so they don't make the same mistakes.

In gift card fraud, everybody but the victim makes money: fraudsters, gift card companies and retailers. The criminals exploit a rapidly evolving payments industry that's shrouded in secrecy, designed to ensure easy transactions and lacking in consumer protections.

The technology companies that provide the infrastructure that enables the gift card economy are privately held and release little information publicly. They facilitate payments behind the scenes, out of the view of consumers who see only the brand name of the card and the drugstore or supermarket where they buy it. While retailers who sell gift cards could do more to thwart fraud, the secretive technology companies that set up and manage gift cards are best positioned to stop rampant criminality, but they don't. There's no legal requirement to do so, and they make money off the crime.

Call this number

When Mae called the number that appeared on her screen, a man answered and identified himself as Mac Morgan, an "Apple high security technician." He gave her his employee ID number, which she dutifully wrote down. The problem seemed to originate from her bank, he told her. She volunteered that she banked with M&T, a Northeast bank headquartered in Buffalo, N.Y. Call them, he said, and provided a phone number.

The woman who answered said her name was Alivia, from the M&T Bank Fraud Unit. Alivia told Mae that a European pornographer and scammer had tried to gain access to her account and withdraw $20,000 during the night. A hold had been placed on the withdrawal, but Mae needed to come down to the bank and retrieve the money before the fraudsters did.

Anxiety rising in her voice, Mae told the woman she hadn't even had a cup of coffee yet; she still had curlers in her hair. Alivia advised her to remove the curlers and, soothingly, promised to stay on the phone with Mae through the entire process.

Sophisticated schemes

Gift cards are just the latest in fraudsters' seemingly unlimited arsenal of tools that help them steal money from people through deceptions like romance scams, fake IRS notices and phony investment schemes. In addition to consumer swindles like the one that targeted Mae, gift cards, including those that are reloadable, have also been hit with an epidemic of card draining, where criminals either steal barcodes from gift cards on the rack or swap in new barcodes they already control.

When consumers put money on a compromised card, the criminals are alerted because they are monitoring the barcodes using automated online account balance inquiries. They can repeatedly check the balances on thousands of barcodes at a time. As soon as money hits a card, the criminals use the account number to purchase items online or in stores, using runners or "mules" to physically go into stores.

The gift card draining problem is widespread enough that it attracted the attention of the Department of Homeland Security and sparked hearings in the U.S. Senate in April 2024. Two months later, Maryland passed the nation's first law targeting card draining, which mandates secure

packaging aimed at thwarting criminals who steal or tamper with the numbers on gift cards.

People ages 18 to 49 are more likely than older adults to lose money in gift card fraud, but adults over the age of 80 lose three times as much as younger adults. The average reported amount lost is $1,000, but more than 100 consumers have reported gift card fraud losses to the Federal Trade Commission in excess of $400,000 each between 2021 and 2023, according to information provided by the FTC through a public records request.

Falling victim to a financial scam ranks second in American fears about criminality, after identity theft, far exceeding concerns about violent crime, according to Gallup. Despite these fears, there doesn't appear to be an accurate government number on exactly how much financial fraud is taking place. The gift card and reloadable card industry also doesn't keep data on the amount of money consumers lose through the criminal use of its products.

At the same time, many gift card companies are not publicly traded. As such, they aren't required to file quarterly or annual financial reports with the U.S. Securities and Exchange Commission, which would indicate the size of the industry and might outline the amount of fraud, among other risks. Consequently, nailing down an exact figure for the total amount of fraud involving gift cards and reloadable cards is challenging.

To track trends, regulators rely on victims self-reporting to gauge the scope of the problem.

Yet the vast majority of people who fall victim to financial scams never report their losses to law enforcement. Most victims are too embarrassed or pessimistic about their chances of recouping losses and so don't

complain. And often they are concerned that their adult children, caregivers or authorities such as adult protective services might conclude that guardianship or institutionalization is necessary to protect them. While it is extremely difficult to know how many elders report financial fraud, a 12-year-old study that's still commonly cited, including by federal authorities, estimates it at 4.2%.

About $550 billion is added onto gift cards annually in the U.S., according to Jordan Hirschfield, a gift card analyst at Javelin Strategy & Research. He estimates that between 1% and 5% of all gift card sales could be fraudulent in some way, but because no one keeps track, it's difficult to arrive at an exact number. If the 1% to 5% figure is correct, the amount of fraud is between $5.5 billion and $27.5 billion per year.

A victim's fear bubble

Mae had entered what AARP calls a fear bubble, an induced state of panic that makes rational thought difficult, if not impossible. This is a greater risk for seniors, because as people get older they experience anger and fear more vividly. The fraudsters who manipulate this panic describe putting their victims "under the ether." Frightened beyond reason, the victim is manipulated into transferring large sums of money to the fraudster to ward off the conjured danger.

Anyone can fall victim. In February, a former New York Times business columnist wrote about losing $50,000 in a fear-induced scam. Mae had graduated summa cum laude from an elite private university. She is a no-nonsense retired nurse and lives independently. Now she was rushing, panicked, to her bank at the direction of a fraudster.

As Mae drove, Alivia advised her to ready a story in case the teller balked at giving her the money. Mae decided to tell them that she needed the $20,000 to buy a used car and it was a matter of urgency.

Frictionless and anonymous

Gift cards have experienced rapid and immense growth because they're a win-win, an innovative convenience for shoppers and a threefold boon for retailers. The gift card racks are mini billboards for retailers.

Consumers commonly spend one- to two-thirds more than the actual value of the card when they use it, said Ben Jackson, chief operating officer for the Innovative Payments Association, one of several trade groups that represent the industry. And sometimes consumers don't spend the gift cards. Terms and conditions of the gift cards, frequently in small print or available only online, may allow retailers to retain the balance after a minimum of five years. It's a tidy gift to retailers amounting to billions of dollars.

The National Retail Federation routinely ranks gift cards as the No. 1 thing shoppers plan to buy. "You don't want friction in your gift giving," Jackson said.

He has traced the first gift card to a glove company in Oregon in 1908. The company extolled the convenience of this new innovation: "Gift givers need not worry about picking the right size or color glove; give the recipient a card and let them choose for themselves."

In the modern era, plastic gift cards were created by Neiman Marcus, but movie rental company Blockbuster first displayed the cards for customers. Known as a closed-loop card, it can be spent for goods only from that particular retailer.

In contrast, open-loop gift cards can be spent at multiple retailers and often have a credit card logo from companies such as Visa or Mastercard, but they don't offer the same protections afforded actual credit cards, such as requiring an ID on file for the card. Some open-

loop cards identify as debit cards even though they also lack the fraud protections of bank debit cards. If the money is swindled, there's no obligation for the company to reimburse the cardholder.

Open-loop cards work everywhere debit and credit cards do and can sometimes be reloaded with funds. Purchasers can pay by cash to remain anonymous. Criminals love them. In the places where fraudsters lurk—on the dark web, which is made up of sites that resemble ordinary websites but are accessible only using special browsers or authorization codes, and on Telegram and Discord messaging apps—open-loop and closed-loop gift cards are offered as payment for everything from payroll to the purchase of equipment needed to perpetrate more frauds.

The first open-loop card originated with retail malls and foreshadowed how the gift card industry would later game regulators. In 2004, Indianapolis-based Simon Property Group and Bank of America created a stored-value card that could be spent at any store in the 159 Simon malls throughout the U.S.

The card activation fee was as much as $6.95. Simon also deducted a fee when a card went unused for six months and charged 50 cents each time a customer checked the card balance after the first inquiry. The fees ran counter to the consumer protection laws of some states where Simon operated, and three states sued Simon.

But the mall operator successfully contended that because it was working with a national bank, federal law and regulations, which had no restriction on these fees, preempted state law to allow the fees. While the cards failed to stop online shopping from eclipsing the American mall industry, it eventually roused federal lawmakers into limited action.

Meanwhile, another gift card innovation had launched in California. In 2002, an in-house unit of Safeway supermarkets looking to sell

nontraditional goods to Safeway customers created the gift card kiosk. It was so successful that a year later the unit became a Safeway subsidiary called Blackhawk Network. By 2007 there were Blackhawk kiosks in 60,000 retail locations, projecting sales of $100 million that year. Seven years later, Safeway spun off Blackhawk as a stand-alone public company.

And in 2018, with help from Blackhawk insiders, a private equity firm called Silver Lake Partners and a hedge fund named P2 Capital Partners took the company private in a transaction worth $3.5 billion. In 2023, Blackhawk Network Holdings had an estimated annual revenue of $2.8 billion.

Blackhawk and its main competitor, Atlanta-based InComm Payments, put cards in drugstores and supermarket chains throughout the U.S. Each card is a separate, private bespoke agreement negotiated between the card owner and the distributor, according to Jackson.

Typically, the distributor negotiates a small discount, usually under 10%, off the card's face value. The discount is split between the distributor and the store selling the card.

The distributor handles card activation so that a retailer like Target will recognize that the card is active in the available amount. In some cases, the distributor also handles the back-end technology that allows consumers to spend the money loaded on the card.

Starting as a small industry a little more than 20 years ago, the closed- and open-loop gift card business has become a massive enterprise involving hundreds of billions of dollars, a festival of frictionless commerce that is also beloved by criminals for its convenience and anonymity.

Mae gets stubborn

The bank teller tried to dissuade Mae from withdrawing $20,000 in cash. Eventually, the bank manager joined the conversation and suggested she take a cashier's check instead. Mae insisted that the guy selling her the car had demanded cash. After about 15 minutes, she wore them down. They gave her the cash.

The bank manager followed Mae to her car to ensure she was OK and to try one more time to get her to reconsider. Mae waived the manager off. Once she was alone again, Mae picked up the phone. Alivia had remained on the line the entire time but told Mae to leave her cellphone in the car while she went into the bank.

A patchwork system of help

In Maryland, the banker had no option but to hand Mae her money. That's not the case in other states. In Florida, a state that contends with elevated incidents of fraud on seniors, the Legislature passed a law in May allowing financial institutions to delay disbursements or transactions of funds to people over 65 if there is a well-founded belief that they are being exploited. In return, the banks receive immunity from any resulting administrative or civil liability.

The delay, which expires after 15 business days, requires that the financial institution launch an immediate review and contact those the account holder has designated as people of confidence. A court may shorten or extend the length of the pause. Anecdotal evidence from law enforcement suggests that even a few hours of delay can pop the fear bubble fraudsters create.

As soon as the persuasive ether of the fraudster lifts, most people realize

they've been scammed. A delay also makes time for the target to talk to someone they trust who might dissuade them from parting with their money.

In New Jersey in 2021, state Sen. Nellie Pou sponsored a bill that proposed a 48-hour delay before using or validating a gift card worth more than $100 and proposed extending the protections to gift cards that credit cards receive under federal laws and regulations: If a consumer reported fraud, the funds would be frozen, and if the fraud investigation were upheld, the money would be returned to the customer. The bill also proposed a fraud incident hotline for consumers, exempted small businesses and levied a $1,000 civil penalty for card issuers that violated its provisions.

The Innovative Payments Association lobbied against the New Jersey bill. The legislation would harm New Jerseyans, it wrote lawmakers, by "discouraging gift card providers to issue and sell such cards in the state." The association argued that the waiting period "defeats the purpose of having a gift card," which is to allow the recipient "to go out and get what they want/need immediately." The legislation passed the state Senate but died in the Assembly and wasn't reintroduced.

Several states have also passed or are considering laws requiring retailers selling gift cards to post warning signs, including Delaware, Iowa, Nebraska, Pennsylvania, Rhode Island and West Virginia, but none go as far as the New Jersey bill.

Waiting periods and warning signs are not the only tools that gift card companies could use against fraud. The distributors already have a technology in place that would be even more effective: velocity limits.

If unusually large numbers of gift cards are being purchased at a drugstore or supermarket, for instance, a distributor like Blackhawk

could freeze the sale and alert the retailer. They have done this on occasion, but our investigation shows this does not happen with consistency. If sale freezes and alerts happened consistently, consumers would be less likely to be reporting on the FTC database large amounts of money lost to gift card scams.

Gift cards could also be required to use geofencing. If a card is purchased in Maryland but redeemed on the same day in California or China, that could be a red flag for fraud because the likelihood that someone like Mae would be able to get gift cards to faraway friends or family so quickly is slim. Geofencing would freeze redemption outside a certain geographical area.

And more simply, retailers could require that gift cards be purchased with a credit or debit card rather than cash to make it easier to reimburse a customer in the event of fraud.

In 2022, around the same time New Jersey was trying to rein in gift card fraud all by itself, Congress passed the Stop Senior Scams Act. The bill created an advisory group of industry members, regulators and law enforcement that is run by the FTC and tasked with studying ways to curtail fraud. Included in the mandate was a focus on technology. The advisory group created a Technology and New Methods Committee subcommittee with about two dozen members, including Blackhawk and the Innovative Payments Association.

In the two years since the bill was passed, the main committee has met only twice. Recommendations by federal advisory committees are not binding. Although the Federal Advisory Committee Act requires that committee meetings be open to the public and their records available for public inspection, it's not a requirement for subcommittees.

The committee is aiming to disrupt fraud, particularly among older

adults, by more efficiently sharing information, data and other intelligence, according to committee member Jilenne Gunther, national director of AARP's public policy institute.

The industry has pushed consumer education as the best response to the gift card fraud epidemic, even as signage and public service announcements have shown questionable effectiveness. "Consumer education … puts the burden of protection on the targets of fraud," Marti DeLiema, assistant professor of social work at the University of Minnesota, testified at an Elder Justice Coordinating Counsel hearing in 2022. At the same time, "fraud targets are often in states of emotional distress."

Some retailers are also training their cashiers to be alert to seniors inexplicably buying fistfuls of gift cards, but these efforts are not always standardized across the industry. Expecting a clerk earning minimum wage to prevent a fearful senior from legally buying gift cards is likely unrealistic.

Blackhawk did not respond to multiple requests for interviews and declined to answer emailed questions. InComm Payments declined to make anyone available for an interview and did not answer detailed emailed questions.

In its letter opposing the New Jersey bill the Innovative Payments Association argued that the industry was "highly regulated," required to adhere to federal requirements and "strict federal anti-money laundering regulations."

In practice, that's not the case.

The criminals direct Mae to crypto

Before sending Mae to buy gift cards, the fraudsters tried another scheme. Alivia directed Mae to a Shell gas station with a Cash2Bitcoin ATM inside and told her that if she put her money into crypto it would be safe. Mae had never before seen a Bitcoin ATM. Alivia talked her through registering for an account, including uploading her driver's license, a know-your-customer requirement that doesn't exist for gift cards.

As Mae fed thousands of dollars into the machine, another elderly woman stood behind her impatiently. I need to get money to send to my nephew, she told Mae. Much later, Mae would realize that the woman was probably being scammed, too. At $15,000, the ATM hit its limit on deposits. The money Mae was feeding into the ATM went flying. She jammed the receipts into her purse and hurriedly gathered cash off the floor.

The fraudsters then sent Mae to the area's two other crypto ATMs, but neither worked. It was 5 p.m. and getting dark. Mae hadn't eaten all day. Alivia asked if Cash2Bitcoin had sent her a receipt for the $15,000. No, Mae replied, forgetting she had shoved it into her purse. Alivia told her to call and find out what the holdup was. Mae's phone conversation with Cash2Bitcoin was concerning enough that the man at the exchange froze Mae's money.

Stymied, Alivia handed the call off to her "supervisor," Mike Ross. Faced with a crypto dead end, but unwilling to relinquish a chance at the remaining $5,000, Ross directed Mae to a Rite Aid near her house to buy gift cards.

Loopholes and laggards

Gift card companies can make the claim they are "highly regulated" because of legislation that occurred after the 2008 financial crisis. The

uproar after Simon Property Group flouted state consumer protection laws led Congress to pass the Credit CARD Act in 2009. The law eliminated many of the garbage fees on gift cards and prohibited cards from expiring for at least five years. It also encouraged states to legislate their own reforms by allowing state law to preempt federal law. But the law didn't extend existing credit and debit card consumer fraud protections for gift card purchasers.

As part of the wave of financial reform, Congress also created a single regulator for consumer financial protection: The Consumer Financial Protection Bureau. It removed regulation-writing authority from the Federal Reserve and gave enforcement and rule writing authority solely to the bureau. It also took away examination and enforcement of all nonbank financial products from the Fed, the FDIC and the Office of the Comptroller of the Currency. Federal consumer protection—bank or nonbank—would ostensibly now be regulated only by this new single regulator.

In the 15 years since the Consumer Financial Protection Bureau was created, there has been a rise in consumer financial products outside of banks, but the new agency hasn't kept up. As part of the rules it issued in 2016 and 2018, it exempted most gift cards, open- and closed-loop alike, from regulation.

While the bureau declined multiple requests to explain why gift cards were exempted from its consumer protection rules for fraud, it did point to resources including a flowchart showing what types of electronic payment methods would be covered under its rules. The chart, a near-incomprehensible tangle of arrows and scenarios, shows how most prepaid gift cards are exempt from the fraud consumer protection regulations common for debit and credit cards, including all gift cards and branded reloadable cards purchased in retail drugstores and supermarkets. This exemption exists even though these prepaid cards

rely on electronic activation and maintenance, which is the purpose of existing laws such as the Electronic Fund Transfer Act.

The FTC's authority

Aside from the Consumer Financial Protection Bureau, the FTC and the Treasury Department have responsibilities that could protect consumers like Mae from gift card fraud. Yet, to date, their actions concerning gift cards are spotty at best.

The FTC is the original consumer protection agency. It can regulate "unfair or deceptive" acts or practices in commerce and provides annual statistics of consumer reports of fraud in all products and services. It provides advice about avoiding scammers, and consumers can fill out a form and join other tragic stories in a growing database, but there is little consequence for the companies involved. The FTC contends it has jurisdiction to bring enforcement actions against gift card nonbank entities for unfair or deceptive acts or practices, but the last time it appears to have done so was in 2007.

The FTC provided a background interview and sent a follow-up memo, but it declined to answer questions about the differences between its authority and that of the Consumer Financial Protection Bureau, or confirm which agency is the primary federal regulator of gift cards.

More agencies, little oversight

The Treasury could also get involved. Two agencies of the U.S. Department of Treasury tackle fraud that touches on national security, terrorism and transnational gangs. Increasingly, criminals from China, Iran, North Korea, Russia and the occupied areas of Ukraine target Americans with tacit, and sometimes explicit, state support. These

Treasury agencies have also largely given gift cards a pass, exempting them from controls in place to combat these crimes, even though there is evidence that the cards are being used by international criminals.

The Financial Crimes Enforcement Network, a bureau of the Treasury Department, requires two types of reports that can involve gift cards: currency transaction reports for transactions of $10,000 or more that are made in cash, and confidential suspicious activity reports for a variety of transactions of any value that the filer considers suspicious, including suspected elder financial exploitation.

Financial institutions, including banks and businesses such as car dealerships, casinos, antique dealers and money service providers, are required to file the reports. These include money transmitters—companies such as Western Union and MoneyGram—that work through retail establishments such as supermarkets and Walmart to send money overseas or to another city rather than using a bank wire transfer.

Those businesses must obtain personal identification information, such as a Social Security number and driver's license from the person conducting the transactions, for the report. Financial institutions file millions of reports every year.

In 2011, with gift cards still in their infancy, the Financial Crimes Enforcement Network issued a regulation to amend the money service business definition to address prepaid access products such as gift cards.

But despite law enforcement concerns, the agency exempted open-loop cards up to $1,000 that weren't used internationally and closed-loop gift cards up to $2,000 from the money-laundering regulation. For closed-loop cards, there was no restriction on international use.

The Financial Crimes Enforcement Network also didn't limit aggregation for gift cards. Banks and money service businesses are generally required to aggregate transactions made on the same day from multiple locations and must report if the total amount goes over $10,000 for the day. For gift cards, however, there is no aggregate tracking requirement, so fraudsters can direct seniors to multiple stores in a day—even stores from the same chain—to buy $2,000 worth of gift cards at each, racking up tens of thousands of dollars.

The Financial Crimes Enforcement Network's rule specifies that "categories of prepaid access products and services were exempted because they pos[ed] lower risks of money laundering and terrorist financing," despite noting that law enforcement disagreed.

In response to our detailed questions, the Treasury's Financial Crimes Enforcement Network declined to say how many, if any, regulatory examinations it or the IRS on its behalf has conducted of gift card providers. "Any information or statistics that we can share publicly are located on our website," Financial Crimes Enforcement Network spokesperson Steve Hudak wrote in an email that also included resource links. "FinCEN declines further comment."

The final agency in the gift card regulatory puzzle is Treasury's Office of Foreign Assets Control, which administers and enforces economic sanctions programs against countries and groups of individuals, including foreign hackers and fraudsters targeting the United States.

But because gift card purchasers don't have to show identification and can provide the card number or a text picture of the card to someone overseas, gift card companies can't prevent sanctioned people, groups or nations from using their products.

Only one enforcement action appears to have been taken by the Office

of Foreign Assets Control against a gift card provider.

In 2022, when Tango Card products, now a division of Blackhawk, self-reported that cards had been used to purchase goods or services in malign nations, including Iran, North Korea, Syria and Russian-occupied areas of Ukraine, the bureau sanctioned the company $116,048.60.

The Office of Foreign Assets Control did not respond to repeated requests for comment.

Mae sends the police away

At Rite Aid, Ross instructed Mae to purchase three types of gift cards: two $500 Nordstrom cards, two $500 Target cards and one $200 Macy's card.

Given the size of the purchase, the Rite Aid cashier called over the manager. Mae lied and said she needed the gift cards for her grandson. Likely due to the $2,000 limit Rite Aid imposed on daily purchases of closed-loop gift cards, the drugstore would sell her only the four Nordstrom and Target cards for a total of $2,000. Back in her car, Mae scratched the back of the cards to reveal the numbers and read them to Ross.

He was about to direct her to the next stop when there was a knock on the car window. It was a police officer. Mae had been scheduled to cook dinner for a gentleman friend who had become worried by her absence and contacted the local police. They'd tracked down her car. Ross told her to get rid of the cop by inventing a story. He'd stay on the line to listen. She rolled down the window and did as Ross instructed, reassuring the officer that all was well, and she'd be home soon.

When the policeman left, Ross sent Mae to a nearby Food Lion

supermarket to buy more gift cards. The Food Lion was close to Mae's house, and the store manager knew her. He refused to sell her the gift cards. This is a scam, he told her. It was now almost 8 pm. Resigned, Ross instructed her to go home but not tell anyone what had transpired.

The fear bubble lifts

By the time Mae pulled into her driveway, the ether had lifted and she knew she'd been scammed. "It was a big fat light bulb: "You've been screwed,'" she said.

Mae called M&T and learned there was no open fraud case. She called Target. Only 30 minutes had elapsed since she purchased the gift cards at Rite Aid, but they'd already been spent.

Recent prosecutions of Chinese gift card draining rings have revealed that the criminals employ networks of mules. These low-level employees are already positioned to buy goods in person once gift card numbers are obtained. And there are other avenues to monetize the gift cards besides an army of low-level buyers. On the Russian-owned Telegram app, dozens of gift card marketplaces sell illegally obtained cards. The traffic in illicit gift cards appears to be growing in popularity because it's possible to move huge sums of money offshore anonymously with little to no regulatory controls.

"The reduced fraud protection makes it easy for cybercriminals to find buyers," said Ensar Seker, advisory chief information security officer at SOCRadar, a cybersecurity firm that monitors the channels.

The cards are usually sold for 50% to 75% of face value, based on the risk incurred in obtaining them, according to Seker. If cards need to be moved quickly because they were acquired through hacking and likely to be canceled, they're worth closer to 50%. Cards obtained by fraud are

worth closer to 75%, because there is little risk of being caught for using one.

Retailers aren't required to know who their customers are. So the retailer issuing the card has no idea whether the cardholder is the person who bought it, someone who was gifted the card, a fraudster or someone who purchased it from a fraudster on Telegram or the dark web. Sometimes criminals will report the cards stolen and receive a new number to cover their tracks. Because the retailer doesn't know who bought the card, it can't tell that it's the fraudster making the call.

Increasingly, cryptocurrencies can be traced and recovered, said Seker, but gift cards cannot.

"The most important aspect for the criminal is to stay anonymous and untraceable. Gift cards allow this," he said.

Epilogue

Investigators tried to pursue the criminals responsible for scamming Mae. Her case was referred to a special elder financial exploitation team. Investigators met with Mae less than a week after the fraud.

The phone numbers the fraudsters used in speaking to Mae were internet lines from a service provider that had little information to offer and denied any responsibility. The phone service had been purchased using an open-loop gift card, so there was no record of who purchased the service.

Mae had thrown out the gift cards but gave the investigators the Rite Aid receipts, which had partial numbers of the gift cards, similar to ATM receipts. The investigators subpoenaed Rite Aid for the full gift card numbers using the postal mailing address the store provided for

subpoenas.

After a substantial delay, Rite Aid responded to the subpoena, claiming it couldn't provide the full card numbers using its point-of-sale records. Investigators later connected with a regional loss prevention manager at a different store who provided the full gift card numbers that Rite Aid corporate headquarters claimed in its subpoena response it didn't have.

The investigators then subpoenaed Nordstrom and Target. But by that time there was no information left to provide. Store surveillance footage was months gone, overwritten with new footage. The retailers had no records of who had used the cards. So despite immediate action by law enforcement, the criminals had vanished, along with Mae's $2,000.

Mae got most of her bitcoin money back, thanks to the compliance efforts and fraud freeze that had been placed on her bitcoin account on the day of the fraud.

Even as fraud against the elderly, including through gift cards, continues to grow, it's primed to get only worse. In 2023, Americans 65 and older represented 17.3% of the population, about 57.8 million people. By 2040, they will be 22% of the population, numbering more than 78 million. By 2060, that number is expected to be 88.8 million.

These seniors will be sitting on nest eggs accrued over a lifetime, and fraudsters want a piece of it.

Mae reported her story to the local police, AARP and the FTC database. "It can happen to anyone," she said.

Provided by The Conversation