Illustration: Zach Hackman for Bloomberg Businessweek

Businessweek | Crypto

Drug Cartels Are Shifting Their Money Laundering to Crypto. Cops Can't Keep Up

A vast ecosystem supported by the gig economy has sprung up to clean all that cash.

By Jessica Brice

February 11, 2026 at 5:00 AM EST

Save Translate

The pitch was simple: Crypto for "cold hard cash." No names. No questions asked.

David Scotese posted his ads online, but the transactions played out in the open, at Victory Park in Murrieta, California. The park was the heart of the community. Soccer games on the lawn. Birthday parties in the shade of a gazebo. And there in the parking lot, Scotese in a 10-year-old maroon Honda Accord.

Listen to the Story

Drug Cartels Are Embracing Crypto and Fi

00:00 / 33:59

In person he was an unassuming suburbanite with wire-rimmed glasses and neatly parted hair. But on LocalMonero.co, an online matchmaker for buyers and sellers of Monero, a so-called privacy coin, he was LetterGuy21969. It was at Victory Park that his offline life and online alias converged.

From at least 2021 to 2023, the US Department of Homeland Security says, Scotese ran his illicit business out of that parking lot, taking in cash and paying out the equivalent in crypto, minus a little something for himself. Southern California is a main artery for the fentanyl trade—was that where the money came from? He didn't know and didn't want to. He also accepted cash by mail, according to DHS, and conducted more than 4,000 no-paper-trail transactions for clients he knew little to nothing about.

"Sometimes I feel that I'm too comfortable with this, doing such large amounts of money," Scotese pondered after receiving $60,000 in May 2023 from an undercover agent. "It's going to hurt me someday." The following month he was arrested.

Scotese near his home in Murietta, California. *Photographer: Alex Welsh for Bloomberg Businessweek*

Cash handoffs like the one at Victory Park have been playing out across the US in recent years. Just outside Boston, an agent accepted $140,000 in bundles of 10-dollar bills behind an apartment building and dropped the equivalent minus commission into a Colombian broker's crypto wallet. An FBI operation in Kentucky took control of a crypto dealer's dark-web account and flipped one of his mules, who then wore a wire during 80 cash pickups worth more than $15 million. And in a sting that stretched across the eastern half of the US, freelance couriers handed off boxes and bags of cash—almost $2 million in a dozen parking lot meets—to undercovers posing as crypto dealers.

This, law enforcement officials say, is what money laundering looks like today, with participants ranging from low-level gig workers such as Scotese to more ambitious brokers working for Chinese networks and orchestrating cash pickups across several cities. These people trade in a range of cryptocurrencies, as well as more traditional laundering techniques, basing their offerings on the risk of the trade

and what the client needs. Bitcoin is still popular as the most liquid, most widely accepted and most deeply embedded cryptocurrency in the underground economy. Monero is built for anonymity, because transactions are almost impossible to publicly trace to a user's wallets. Tether on the Tron blockchain offers rock-bottom fees (often around a dollar) and lets a user split transfers into hundreds of tiny fragments with minimal oversight.

Powered by encrypted messaging apps, anonymized platforms and a growing pool of people willing to move money for a cut, the system is agile, scalable and disturbingly hard to shut down. What began a decade ago as a fringe trend on dark-web bazaars is fast evolving into a sprawling global ecosystem of freelance money movers. Even the biggest criminal groups, long reliant on in-house laundering, are starting to tap it. "Inside law enforcement, it's well known we're underprepared for these massive changes," says Derek Maltz, former acting administrator of the Drug Enforcement Administration, who stepped down last May. "As I was on my way out, one of the things that stuck with me was just how complex these money laundering cases have become. Anyone who tells you law enforcement's got this, they're not being honest with you."

This is happening while the Trump administration is shifting funding and priorities away from money laundering investigations while also clearing the way for crypto to take a larger role in global finance. That raises the dangerous possibility that laundering operations could slip entirely beyond the government's ability to police them, several watchdogs and crypto enforcement agents say.

"So few people understand how this ecosystem really works—even the people passing the legislation," says Scott Greytak, deputy executive director of anticorruption advocacy group Transparency International US. "I don't think this story ends well."

A DECADE AGO, INSIDE THE MIAMI FIELD DIVISION OF THE DEA, Special Agent Lili Infante began pushing an idea almost no one

around her understood. She wanted to build a task force dedicated to cryptocurrency.

At the time, Bitcoin was still widely regarded as internet play money. Infante herself had learned of it a few years earlier from an episode of *The Good Wife* called “Bitcoin for Dummies.” But where others saw a curiosity, she saw a laundering revolution. It offered everything criminal groups craved: no scrutiny, no names, no borders. “I started telling everyone, ‘Crypto’s going to be big,’” says Infante, who was born in Russia and has the white-blond pixie hair and high cheekbones of a video game heroine. “No one knew what I was talking about.”

Infante understood early that the cartels would find use for crypto. *Photographer: Lawren Simmons for Bloomberg Businessweek*

She studied the FBI's takedown of Silk Road, the Bitcoin-based darknet bazaar for homegrown pot and drugs made in basement labs. She led the team that toppled Hydra, a Russian marketplace, also running primarily on Bitcoin, for stolen data and synthetic highs. Then came the flood. Notices from Homeland Security Investigations (HSI) warned that criminal groups in China, North Korea and the Middle East were quietly experimenting with crypto too.

What about the drug cartels?

Infante called an informant: a broker, someone who'd been cleaning cartel money for years. Court documents show that, scattered across the country, some brokers plug into cartel laundering pipelines one day, then slip intel to the DEA the next. "Career informants," the agents call them. These traditional brokers are agnostic, opportunistic, loyal to whoever pays best. Sometimes that's the US government. The upfront fee for information isn't much, maybe a couple thousand dollars. But if the feds seize assets based on the tip, the payday can reach 20%.

"They can make millions," Infante says. "Assuming, you know, they don't get murdered by the cartel first."

The traditional broker playbook involves such techniques as straw accounts and bulk cash smuggling. Her source ran a different old-school scheme known as trade-based laundering: He funneled cartel cash to a US-based importer buying products from Mexico or Colombia. The importer would use the dirty money to overpay for the shipment. The exporter, after receiving payment, would pass the extra money (minus a commission) to the cartels.

Infante asked her informant to offer a different kind of service the next time the cartel needed to clean cash. Skip the shipment. Just trade the money for Bitcoin.

It took six months for someone to bite. A contract to clean $300,000 was arranged. A DEA undercover agent posed as a courier to pick up the cash while Infante and her team watched nearby. Infante swapped it for Bitcoin, sent it to a wallet address provided by the broker, then followed the transaction's trail on the blockchain.

Crypto isn't the digital black hole many people think it is. Every transfer is permanently recorded in a blockchain—a public digital ledger stored across thousands of servers worldwide. The FBI or DEA may not know who's behind a wallet today, but if they can get a break—the right tip, the right seized phone—the entire financial trail can snap into view. While there are tricks to cover the track—using a tool called a mixer to scramble a transaction's footprint, or privacy coins such as Monero—regulators have cracked down on both fronts, prosecuting major mixers and pressuring exchanges to delist untraceable tokens.

Infante's plan was never to arrest anyone right away. What she really wanted was to identify cartel brokers when they cashed out in Mexico by converting the crypto into pesos and transferring them via banks to someone in the cartel. It played out exactly as hoped, allowing the DEA to map a new rung in the criminal group's hierarchy.

"Compared to other cybercriminals and dark-web guys at the time, they just weren't savvy at all," says Infante, who left the DEA three years ago to found CAT Labs, a software company that searches for crypto keys and wallets on confiscated devices so law enforcement can recover illicit assets. "It was a dream."

But the thrill was short-lived. The cartels remained skeptical and weren't interested in another Bitcoin contract; Infante believes the price volatility of Bitcoin made them nervous. "They didn't care about Bitcoin," she says. "They just wanted to move value from Point A to Point B. And they already had their more familiar routes."

She pivoted her task force to focus on Hydra, the Russian marketplace, which took years to take down.

Nonetheless the cartels had a problem other criminal groups didn't. North Korean hackers, Chinese fraudsters and darknet dealers were used to moving funds with a keystroke. But the cartels had big, physical piles of cash stashed in every US state. The federal government estimates as much as $100 billion a year has to be disguised, absorbed, made to look like it came from somewhere else, then find its way back to the drug bosses in Mexico and Colombia.

When the world shut down in 2020 because of the pandemic, many of the cartels' old cash-based routes crumbled overnight. Restaurants, bars and casinos used as fronts were shuttered, and border traffic slowed. At the same time stablecoins, including Tether, became popular. Unlike Bitcoin, stablecoins are pegged one-to-one to the dollar. The wild price swings weren't a problem anymore. Chainalysis, a blockchain analytics firm, estimates that stablecoins now account for 84% of all illicit crypto transaction volume. (Tether Holdings SA, the company that issues the stablecoin, has said the public nature of blockchains means it's "possible to meticulously track every transaction, making it an impractical choice for illicit activities.")

"It was the perfect storm—the pandemic and stablecoins," Infante says. "Suddenly, DEA colleagues from all over are coming up to me saying, 'The cartel wants to use Tether. What the hell is Tether?'"

AROUND 2018 SOMETHING CHANGED IN THE WAY THE CAREER informants talked to the DEA. Their tone changed. They weren't offering tips anymore—they were venting. We're losing business, they said. Jobs that once paid them 8%, 10%, 15% were suddenly going to rivals willing to do it for 1% or 2%. Sometimes for free. Inside the DEA, agents were seeing it too. "Our undercovers who'd infiltrated networks were suddenly getting outbid," says Christopher

Urben, a former assistant special agent in charge for the DEA and now managing director of Nardello & Co., a global private investigations firm. “They couldn’t get money laundering contracts anymore.”

Who was undercutting them? Who could move money that cheaply and at scale? The answer kept coming back the same: the Chinese.

Former DEA agent Urben. *Photographer: Lawren Simmons for Bloomberg Businessweek*

To investigate this emerging phenomenon, the DEA’s Special Operations Division launched Project Sleeping Giant. Over the following five years it would map not just a new money laundering scheme but also a new era.

Chinese and Mexican money operations had each been evolving rapidly, shaped by government crackdowns and accelerating technology. Rising in the background were dark-web marketplaces and decentralized brokers. These networks had largely moved on parallel tracks. But in the early 2020s, they merged. Dirty cash now feeds into crypto, and crypto back into cash. It's the foundation for a truly global illicit financial system.

Evidence of that rolled into sharper view on Jan. 10, 2021, when Customs and Border Protection snapped a grainy photo of a car as it crossed from Mexico into California. The photo, which was included in a 2024 indictment, shows a 23-year-old named Peiji Tong at the wheel, wearing a Covid mask. In the passenger seat, Edgar Joel Martinez-Reyes, then in his early 40s, slouched low. One man Chinese, the other Mexican. A suspected money launderer and a suspected narco trafficker.

Both were on law enforcement's radar, from separate investigations. So when the odd couple joined the tens of thousands of people crossing the busiest stretch of the US border that day, an alert went out. HSI would later determine the two had been in Mexico to strike laundering deals—contracts to move Sinaloa cartel cash, including through the Chinese network Tong was allegedly a part of.

Two weeks later, according to the indictment, at a parking lot behind a quiet office complex in the Los Angeles suburb of Downey, a task force of federal agents and local cops watched as members of Martinez-Reyes' group—drug dealers, couriers and smugglers—dropped off cash or picked up assignments to clean money. For the most part the group did that in all the usual ways: breaking it into small amounts to be deposited into straw accounts at ATMs around town or buying gold and gems to transport south.

One exchange stood out. When a quarter of a million dollars was delivered inside a big white gift bag with the words "Happy Birthday" scrawled on the side, someone from Tong's group showed

up—not to launder it in the traditional way but to sell it, to clients eager for US dollars.

To the Sinaloa traffickers, those dollars had always been a headache, especially since the Mexican government restricted the deposit of US currency in Mexican banks. But for the Chinese they're the prize. China's government maintains strict currency controls that cap how much money a citizen can send abroad—$50,000 a year, per person. To get around that restriction, millions of Chinese nationals rely on a shadow banking system that can deliver US dollars on demand.

That, say federal agents, is why Tong's network and other Chinese brokers could so easily outbid their rivals. The cartels weren't the clients—they were the suppliers. Their dirty money was the product. The customers of the Chinese brokers, who ordered dollars over the WeChat messaging app, were willing to pay premiums of 30% or more, according to two federal agents who asked not to be identified because they weren't authorized to speak publicly.

Over the three years that agents worked this leg of the operation, they seized $2.8 million in dirty money and surveilled 18 more cash drops they let go through while gathering evidence. In April 2024 the US Attorney's Office in the Central District of California indicted Tong, Martinez-Reyes and 22 other people. Tong fled to China, and Martinez-Reyes is out on bail awaiting sentencing after pleading guilty to operating an unlicensed money transmission business and conspiracy to distribute cocaine and meth.

One of the clearest examples of the potential for this new marketplace for black-market dollars came on the casino floor. In 2024, Wynn Las Vegas agreed to forfeit $130 million to settle criminal allegations after admitting in a so-called non-prosecution agreement that it had worked with a web of unlicensed brokers to quietly deliver cash to high-rolling Chinese gamblers.

The collaboration between Chinese and Mexican gangs has also, according to Urben, accelerated the use of so-called mirror, or "flying-money," transactions. These involve parallel swaps: A cartel provides cash to Chinese brokers in the US; the Chinese arrange for something of equal value—either crypto or chemicals the cartels need to make fentanyl—to be sent directly from China to Mexico. In this way they get closer to their fondest dream: bypassing the formal financial system altogether.

OPEN YOUR PHONE. SCROLL THROUGH YOUR APPS. ONE DELIVERS your dinner, another your groceries. Someone to walk your dog. Not long ago, trusting people you didn't know for many of these tasks would have sounded insane. But then came Uber, and you started hopping into strangers' cars. Airbnb got you to sleep in their beds.

That same dynamic now shapes the black market through Signal, Telegram and WhatsApp. These apps are encrypted—often end-to-end, meaning that messages sent through them are scrambled and unreadable, except by the sender and recipient. It's hard to overstate how profoundly that has supercharged and fortified criminal enterprises, law enforcement says. For decades police and federal agencies could get a wiretap and listen in as criminals plotted meetups and cash drops. They could hop from phone to phone until they'd mapped an entire network. That's largely a dead end now—there's no clear legal framework authorizing the use of spyware to intercept end-to-end encrypted messages in real time, even with a warrant.

WeChat goes further, as does Weixin, its counterpart for users with a number from mainland China. These apps combine voice and messaging with payment systems and social networks, all of it on a single platform owned by the Chinese company Tencent Holdings Ltd.

Almost nothing in law enforcement's tool kit works in the face of WeChat. Seizing a single phone in a traffic stop—the next best option now that wiretaps are out—yields little, because Tencent generally doesn't reveal the identity of the people behind a WeChat account or the account's contacts. Trying to pull financial records is difficult too: The company says it can't cooperate with a US investigation or hand over any information without a formal request from the Department of Justice that is approved by the government in Beijing, in the case of Weixin, or Singapore, where WeChat is based. As for sending in an undercover, WeChat's built-in social layer gives brokers a track record and shared contacts. An outsider can't just show up and start running deals.

"The fact that the Chinese have this system, it's a huge advantage," says Urben, the former DEA assistant special agent in charge of Sleeping Giant. "You can't wiretap the network. You can't infiltrate it. You're back to doing street-level surveillance, grabbing people one by one and trying to flip them."

Now swipe through your banking apps. This is where the next seismic shift happens.

You probably have one for the bank that holds your money and another—Venmo or Zelle—for moving it around. They're billed as symbols of frictionless finance, and they work just fine if you're paying rent or splitting the cost of dinner. But try to move money in less predictable ways—say, across a border or into crypto—and those same apps start throwing up hoops and hurdles. That's by design, and it's the point in the app-based ecosystem where criminals still struggle.

But even that's changing. Getting money into the formal financial system without setting off alarms and triggering an investigation has always been the single biggest point of friction in criminal operations. Now a convergence of forces—crypto, President Donald

Trump and new banking regulation and legislation—is smoothing that out as well.

Two-and-a-half weeks after Trump returned to office, the House Financial Services oversight and investigations subcommittee called crypto experts to testify on Capitol Hill. Trump had just signed an executive order naming digital assets a national priority, and the Republican chair, Dan Meuser, was eager to give oxygen to claims that regulators had spent the previous four years on a crypto witch hunt.

Inside a cavernous committee room, Paul Grewal, chief legal officer of the cryptocurrency exchange Coinbase Global Inc., offered a familiar refrain: Law enforcement doesn't fear crypto—it loves it. "I encourage you to speak with the men and women of law enforcement," Grewal told lawmakers. "I think they will tell you their best days are when they are investigating crime that involves cryptocurrency as opposed to cash or other forms of payment."

But ask federal agents, officers or prosecutors whether crypto's traceability really makes their jobs easier, and the answer you're most likely to get is: If only.

To follow the money in crypto, investigators need a wallet address, a transaction hash or a private key. To get any of those, they need access to a device or dataset where that information is stored, something they usually can obtain only if they have someone on the inside or they've been following a suspect long enough to get a warrant to seize a phone or raid a stash house. Then they need the tools and training to find the string of seemingly random characters buried in all that data—and the expertise to trace it on the blockchain.

For agencies and police departments that are chronically understaffed and undertrained, that's a big ask. Outside of major cases, they often don't even try. "We just don't have the personnel," says Julie Shemitz, the former assistant US attorney who helped

build the case against Tong and Martinez-Reyes, the Chinese money broker and Mexican narco trafficker. “We absolutely cannot keep up.”

Shemitz put words to a quiet fear that agency chiefs rarely say out loud in Washington. Law enforcement is fighting a new war with old weapons. They’re up against technologies they don’t fully understand, networks they can’t penetrate and legal frameworks that were never designed for what’s coming next.

Trump took office vowing to wage war on drug cartels. He designated them terrorist organizations and slapped sanctions on three Mexican banks accused by the US Department of the Treasury’s financial intelligence unit of laundering dollars.

But behind the scenes the administration is also eliminating resources and dismantling tools needed to investigate money laundering, say several former and current agents and prosecutors, speaking on condition of anonymity because they either aren’t authorized to speak publicly or because they fear retribution. The administration has shut down the crypto enforcement unit at the US Department of Justice that helped federal investigators trace digital assets. Bloomberg previously reported the department also plans to disband its cross-agency Organized Crime Drug Enforcement Task Forces, which played an important role in scores of money laundering and cartel cases, including the arrest of Sinaloa kingpin Joaquín “El Chapo” Guzmán. Meanwhile, thousands of agents from the FBI, DEA and HSI have been reassigned to immigration enforcement or crime control in major cities.

The Justice Department said in an emailed response to questions that the cross-agency task force’s cases have been transferred to a similar program at the Department of Homeland Security, which will carry on the work instead. It also pushed back on the idea that shifting priorities could undermine the fight against money laundering. “Assisting our partners with federal immigration

enforcement has not deterred our ability to adapt to emerging technologies, dismantle the cartels, and successfully prosecute crime to keep Americans safe," it said.

Certainly the department is still indicting money launderers. On Jan. 8, a broker was charged in Cincinnati with coordinating drug cash pickups across the US and delivering the money to clients who wanted to buy the dollars. Prosecutors allege that he used flying-money schemes to transfer the value from China to Mexico, with just one of his ledgers recording contracts worth more than $27 million in 2024 alone.

But the investigation in that case, plus 10 similar ones the DOJ's press office pointed to, would have started years ago, under different guidance. In 2025, in a memo later made public, the department instructed assistant US attorneys nationwide to stop pursuing so-called 1960 cases, named after the federal statute prohibiting unlicensed money-transmitting businesses, against crypto platforms, mixers and brokers. They were told instead to focus on cases tied to priority crimes such as drug trafficking and cartel financing. Several prosecutors say that directive amounts to a de facto ban on many money laundering cases against crypto brokers and services, because 1960 charges have long served as the investigative trigger and a reliable prosecutorial fallback when direct evidence of more serious crimes is too difficult to prove in court.

Meanwhile the real threat—the point at which the last remaining point of friction for criminal groups falls away—has yet to play out. Until now, crypto has largely functioned like any other on-ramp for dirty cash. Criminal groups swap illicit proceeds for digital assets, transfer value across borders and then eventually convert those assets back into cash or bank deposits. This reliance on regulated financial institutions—where US anti-money-laundering enforcement is concentrated—is the window law enforcement uses to keep tabs on illicit flows.

Trump's stablecoin legislation, known as the Genius Act, establishes a regulatory framework under which licensed nonbanks can issue dollar-backed digital coins that can be used for instant, borderless payments—no traditional banks required. Supporters say the law brings crypto into the regulatory fold, while also enhancing the global standing of the dollar. Transparency International cautions that it sets the stage for a parallel, opaque financial ecosystem that illicit actors can exploit by using foreign stablecoins and circulating billions on private ledgers, leaving no trace on public blockchains and no path for regulators to follow.

The great fear among law enforcement is that illicit actors will someday be able to conduct all their business in crypto without ever converting it to cash or bank deposits. "That's when the genie is really out of the bottle," says former FBI analyst Nick Carlsen, who is now a senior investigator at crypto tracing firm TRM. "We're not there yet, but we're getting close."

DAVID SCOTESE LIVED JUST TWO BLOCKS FROM VICTORY PARK. A self-described voluntaryist—subscribing to a branch of libertarianism based on the belief that every transaction between people should be voluntary and that government is by nature coercive—he ran his brokerage operation like a purist. He'd take either side of a trade so long as the margin worked in his favor.

Scotese says he began buying and selling Bitcoin for a commission in the early 2010s, and the side gig quickly replaced his day job as a software engineer. He started out allowing people anywhere in the US to deposit cash directly into his bank accounts in return for crypto. But that not only raised money laundering flags at banks—it also turned him into the go-to for a number of romance scammers who persuaded victims to turn cash into crypto through Scotese's accounts and then ran off with it. His bank accounts kept getting shut down—Wells Fargo, Chase, US Bank, Bank of America—but he was never charged with wrongdoing.

From then on, he insisted on cash by mail or in person. His name first hit government radars in 2015, when a postal inspection dog flagged an envelope reeking of drug residue. Inside was $15,000, sent by a suspected drug dealer in Florida. The cash was seized. Years passed. Scotese started running his operation out of Victory Park, offering regular business hours every weekday afternoon except the first Friday of the month. According to court documents, this was when he met with other Bitcoin enthusiasts at a local Tex-Mex restaurant.

On an afternoon in June 2023, a little before 1 p.m., he hopped into his car and drove over to the park.

The lot at Victory Park, where Scotese bought and sold crypto, no questions asked. *Photographer: Alex Welsh for Bloomberg Businessweek*

A man in a T-shirt and jeans was waiting near the entrance of the parking lot in a silver Toyota Tundra, parked backward. Scotese pulled in forward to allow the two men to trade window to window.

The man in the truck introduced himself only as Primo (Spanish for “cousin”), and Scotese didn’t push for more. He says he didn’t think it was any of his business.

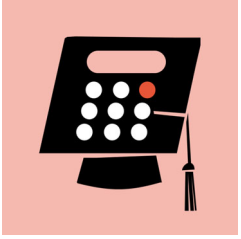
“LetterGuy?” asked Primo, who was really an undercover HSI agent.

“Yeah, I’m LetterGuy,” Scotese replied. “Dave.”

Primo didn’t want to trade window to window—he likely didn’t want to risk a messy recording—and asked Scotese to climb into his vehicle. He handed him $60,000 in cash. That part of the transaction is usually quick. Transferring crypto in return, however, takes at least a couple of minutes. In those uneasy gaps, as the broker and undercover wait for the proof of transaction to pop up on their phones, agents will often try to steer the conversation subtly toward the supposed source of the cash, hoping to establish that the money is illicit so they can use that fact later in court. It’s a delicate dance. They need something incriminating enough for a money laundering charge to stick, but not so blunt that it blows their cover.

According to court documents, Primo alluded to cash stored around the US and floated a bigger offer: Could Scotese handle $200,000 at their next meetup? Scotese hesitated. Until now he hadn’t seemed particularly cautious. But suddenly he pulled back. He said he wanted to meet a couple more times before they went that big.

Scotese hopped back into his car. And then, as he checked his phone and considered popping over to the grocery store, HSI agents and local cops surrounded and arrested him. Nearby, his three-bedroom home was raided. Inside, authorities seized more than $1.3 million in crypto, cash, gold and silver.



Crunch the numbers

Scotese's case was valuable mostly as a message to others: a rare chance for prosecutors to send a public warning. He was just one node plugging into a rapidly expanding and evolving financial infrastructure that increasingly connects hardcore criminal networks and independent brokers. Moreover, by the time agents first watched him in Victory Park, the laundering landscape was already evolving past him. Freelance networks were expanding in every US state, and Chinese brokers were seizing control.

Scotese near Victory Park. *Photographer: Alex Welsh for Bloomberg Businessweek*

“You can go after the guys exchanging $300,000 a pop, but that’s not going to change anything,” Carlsen says. “When you look at a Tether wallet that’s moving money for these big guys, you’re seeing billions. That’s the kind of target you need—not the guy in the parking lot.”

Scotese was arrested on a Friday. By Monday he was released from jail. He was indicted not in California but in New York, where he’d been the target of a separate cash-by-mail case stemming from the

seized $15,000 discovered by the drug-sniffing dog almost a decade earlier. In one of those trades, an undercover agent who went by the alias Gina Monti strategically let slip that one of her dealers was "swallowing more oxy than he was selling." Establishing that a defendant knows money is dirty is required for most prosecutors to support a charge of laundering criminal proceeds.

Scotese eventually pleaded to a lesser charge of operating an unregistered money-transmitting business—the so-called 1960 offense—and was sentenced to time served, plus eight months of probation. Over several conversations with *Businessweek* between November and January, the 56-year-old grandfather was chatty, almost philosophical, about his decade-long run trading crypto and cash.

He acknowledges some of that money might have come from illegal activity. He says he wouldn't have knowingly worked with anyone selling fentanyl, but he also admits he never really tried to screen anyone out. "That's totally on me," Scotese says.

So it goes when money laundering becomes gig work. With every handoff—from dealer to courier, broker to straw account holder—the link to the original crime fades, and it becomes harder for law enforcement to hold anyone accountable.

"I don't think there's any stopping it now," Scotese says. *—With Zheping Huang*

Contact us:
Provide news feedback or report an error

Confidential tip?
Send a tip to our reporters

Site feedback:
Take our Survey

Before it's here, it's on the Bloomberg Terminal