DAILY BEAST

# She was 69. He Was Young, Hunky—and a Fraud.

CYBERGOBLINS

**Love scams hit a record high last year, with fraudsters fooling lonely hearts into sending their life savings in hard-to-recover cryptocurrency.**

*By Kate Briquelet, Senior Reporter and Emily Shugerman, Senior Reporter*
*August 20, 2022*

In May of last year, someone claiming to be a military doctor on a secret mission in North Korea contacted Laura Francis on Facebook, looking for love and connection. Francis, a California realtor, thought he was charming—his profile images portrayed a man with a muscular build, beard, tattoos, and hospital scrubs—but was initially skeptical of his intentions.

The mystery man called himself "David Hodge," and he claimed to be a kind of surgeon, helping soldiers who'd been injured by explosives in war. As part of his backstory, David told Francis he had an ex-wife who had cheated on him, and a 5-year-old son.

David's love-bombing of Francis, 69, was insistent. He texted Francis every morning and throughout the day (usually on Google Hangouts) and called her on the phone just as often. "I fell in love with his voice, he had the cutest laugh," Francis recalls. He serenaded her with links to romantic songs on YouTube: "Hero" by Enrique Iglesias and "I Swear" by All-4-One.

According to Francis, David said “he had been there and done that with the beautiful young women, and they were all not loyal.” He told her he “wanted somebody that was more mature.”

“Meeting you was fate, becoming your friend was a choice but falling in love with you is beyond my control,” David wrote one evening in August 2021, as they discussed buying a wedding ring.

“You have no idea how elaborate it was,” Francis told The Daily Beast in an interview, after she learned her nearly year-long affair with David wasn’t a real relationship but a cryptocurrency romance scam, one in which she claims she lost $248,000 of her savings—money that was supposed to be her daughter’s inheritance.

“He had an excuse or an answer for every question,” Francis said. “I asked millions of questions. Because I didn’t trust or believe anything from the first.”

Anytime Francis doubted him, David would send her photos he claimed were of himself, holding a sign that said: “I love you Laura and am not a scammer I’m Davidson Hodge.” He also sent her a purported passport and copies of a seemingly detailed bank statement, from a local bank in Columbus, Ohio—but which utilized a Chase Bank P.O. Box and which included some notable typos—claiming he had $3 million. He also sent her a photo of his arm, decked in military camouflage, and hand holding an “employment agreement” containing a U.S. Marine Corps logo.

## *“Hunting down your stolen funds can be harder than actually finding true love.”*

Whenever he asked Francis for money, she says, he always promised to pay her back once he was out of the service and had access to his accounts.

David directed her to use several Bitcoin apps including Coinbase and Coin Cloud Bitcoin ATMs until she cut him off in March. (The Daily Beast reviewed some of Francis' Coin Cloud receipts with deposits totaling $37,080 in August 2021 alone, and one blockchain analytics firm said she appeared to have deposited around $60,000 via the ATM in September.)

Asked for comment, Cloud Coin said its terms of service prevent it from sharing personal information about customers but said it has sympathy for the victims of financial crimes. "When a customer buys, the digital asset(s) go into their wallet," the company said in a statement. "From there, we don't know what a customer does with their currency, coin, or token."

Within three months, Francis was sucked into a whirlwind drama rivaling daytime soap operas. And each plot line drew her deeper into what she believed was true love, followed by a rift caused by a second alleged scammer named "Robert Manguire," who claimed to be an oil rig worker in Louisiana and warned her David was a con artist.

"Between the two of them, they had me on the run," Francis said. David would tell her he was shunning her until she blocked Robert, and Robert threatened to tell her family about how much she'd paid David unless she blocked the supposed doctor.

"I didn't know how I was going to face my family," she said, "and I did not know how I was ever going to let my family know how much money I lost."

Romance scams are big business in the U.S., and crypto is a growing piece of it. The FBI reported that Americans lost $1 billion to romance scammers in 2021, while the Federal Trade Commission estimated they lost $750 million to crypto scams that same year. (The FTC also said crypto was the second-most common form of payment in romance scams, above wire transfers and apps like Venmo.) Paul Sibenik, the lead case manager at CipherBlade, a company that helps track and recover stolen or scammed crypto, said anywhere from 30 to 40 percent of his company's clients are victims of a romance scam.

While the FBI began warning about Internet romance rackets as early 2005, the rise of cryptocurrency has made it even easier to scam money instantly, across borders, and without detection. And pandemic lockdowns meant more and more people turned to dating apps and websites as a means of finding love remotely. Romance scams hit a record high in 2021, according to the FTC, totaling more than any other category of fraud.

The horror stories of courtship-based schemes increasingly involve crypto. In February, Nicole Hutchinson of Tennessee told CBS News that she lost $390,000 of her and her father's money—some of it her inheritance after her mom died—after she fell for a scammer named "Hao" on the Hinge dating app. The man encouraged her to create an account on Crypto.com and instructed her to transfer funds to a link he claimed was a cryptocurrency exchange platform; instead, the money went into his pockets.

Another victim, South Carolina business owner Zahra Hajiaghamohseni, told NBC affiliate WCBD-TV that she lost $350,000 after a handsome man wooed her online, then encouraged her to invest in crypto. She later learned her suitor had scammed her, using a fake identity and someone else's photos, after she traveled to an airport to pick him up but he never arrived.

The government has responded to this surge in crypto-related crimes by staffing up with investigators. The Securities and Exchange Commission nearly doubled the size of its Crypto Assets and Cyber Unit this spring, from 30 to 50, and the FBI announced a new Virtual Asset Exploitation Unit dedicated to blockchain analysis and virtual asset seizure. The Justice Department also launched two new crypto-related arms last year: one focusing on criminal money laundering and cybersecurity, and the other on civil fraud cases.

***"You have no idea how elaborate it was. He had an excuse or an answer for every question."***

But the hires do not mean that every crypto fraud will be prosecuted. Several experts who spoke with The Daily Beast said federal law enforcement is unlikely to take cases where it deems the losses "too small"—a label some experts said can apply even to six-figure losses. Victims with smaller losses are directed to local police forces, which often do not have the training or tools to deal with a highly technical crime.

There are other issues that complicate a crypto fraud investigation, the primary one being that the fraudsters could be anywhere in the world—far outside the jurisdiction of local police. They are also incredibly hard to identify, because, although all cryptocurrency transactions are made public on the blockchain, they occur anonymously, identified only by a long string of numbers designating a crypto "wallet." Add to that the fact that many scammers use multiple wallets, or employ something called a "mixer" that combines their money with others to make it harder to track, and hunting down your stolen funds can be harder than actually finding true love.

Going the civil route isn't easy, either, according to Tal Lifshitz, a financial fraud attorney who also handles crypto cases. Tracking crypto transactions often involves expensive software or outside firms that cost more than a recently defrauded litigant can afford. And without those, it's difficult for an attorney to know who to subpoena, or even serve.

"With traditional financial fraud, we know there's a bank [or accounting firm] involved," Lifshitz said. "Even if you don't necessarily have access to it before you bring a case, you know they exist, because they have to. None of those things have to exist in a crypto fraud."

Francis says the first time David asked for money, he claimed his top-secret cover was blown and his military base was forced to relocate. As David and his crew members traveled up a river, he claimed, their boat overturned and they lost their belongings including cellphones. Francis says she paid $5,600 for a new phone for David, and while he was waiting for the device, paid two of his colleagues a total of $7,000 so he could borrow their phones. "He kept

convincing me that where he was stationed and the conditions that he was living under were so dramatic, so iffy, so touch-and-go, we could be dead any minute," she said.

As they began to plan their future together, David suggested she buy her own engagement ring through a military program that would prove he had a fiancée and allow his release from his three-year military contract. She paid a total of $42,568 for a diamond ring—but when the band arrived in the mail, she saw it had a $9.99 price tag and was actually a chintzy cubic zirconia.

The wedding ring wasn't even enough to release David from his military tour, according to him. David told her "Shawn Porter," a colleague he claimed handled the sale of military engagement rings, failed to send "paperwork" necessary to get him out, and the online couple had a fight.

According to Francis, David and Shawn had instructed her to send money incrementally via a Coin Cloud Bitcoin ATM, which she'd visit sometimes three times a day. She says she would feed $100 bills into the machine to send to David as he stood by on the phone to walk her through the process. "It started out at $1,500 a day," Francis recalled. "I got it to $25,000 a day that they allowed me to send. That's how much business I gave that machine."

***"I believed what the guy said, because I guess I wanted to. I wanted to hear the bullshit. I wanted to hear the niceness."***

Messages show that in August 2021, David pushed Francis to withdraw more money from the bank to buy crypto. "Yes honey it's night time here. You can still go to the bank though," he tells her in one message, to which she replies, "I'm not gonna go to the bank and do that David I don't think it's necessary."

She added: “I’m not going to be sending money across the world much longer OK and I hope I don’t have to send any more damn bitcoins ever again.”

Francis also questioned David on whether he was catfishing her, telling him: “I saw women give their whole life savings away to men like you they never met. And they were all deeply in love like I am.”

“No it’s different,” David responded. “They don’t talk on phone they don’t get packages.”

The realtor’s family members, who’d watched her fall deeper into texting David for hours each day, suggested she cut him off and meet someone in person on the dating website Plenty of Fish. That’s where she met Robert, an attractive older man with graying hair.

Francis told Robert that she was seeing someone else, albeit online. “I really, really like him,” Francis says she told him. “But I think he’s lying to me.”

Minutes after Francis sent Robert a photo of David, Robert messaged her with an Instagram profile that revealed David’s photos apparently belonged to another person in real life.

Robert, Francis says, vowed to help her take down the scammer and get her money back. He claimed he could hack Shawn’s Bitcoin accounts and get the $42,000 she’d spent on the engagement ring. All she had to do, he said, was set up an account on a site called Cresco Trading Limited and pay the $37,000 in required fees. (A regulatory body in the U.K. issued a warning about Cresco in September 2021, saying it was “not authorised or registered by us but has been targeting people in the UK, claiming to be an authorised firm.”)

Francis says she paid the initial fee but balked when a purported customer service agent for the site told her she needed to put the same amount of money in her Coinbase account to verify she had the funds. Francis refused, and turned back to David.

The situation only got stranger from there. David, she said, claimed Francis had exposed his identity by talking about him with Robert online. Days later, Shawn messaged Francis and claimed David was arrested and it was all her fault.

“Well, you blew it this time, Laura. David is in jail. They picked him up. Because Robert reported him. And they’re holding him on espionage and treason,” she recalls Shawn telling her.

She says David contacted her from “jail,” crying and claiming he was being tortured in custody. Shawn told her David was only getting one meal a day, and was “suffering a lot,” according to messages reviewed by The Daily Beast. “Robert is the devil,” Shawn added. “He will have David killed if he had his way.”

Desperate to help, Francis returned to Robert, and begged him to recant his report. At David’s urging, she even paid him the $56,000 he demanded to do so. At the same time, Robert sent Francis an email with a photo lineup from a law enforcement agency’s “wanted list”—apparently Photoshopped with Francis’ picture—warning that if she continued to associate with David, she’d end up on authorities’ radar.

“I hope you listen this time or you end up behind bars,” one September 2021 email reviewed by The Daily Beast read. “If you disclose this to anyone you’re in for a big trouble.”

To this day, Francis says, she doesn’t know how Robert found her on Plenty of Fish. She didn’t tell David she was moving on to the dating site, but says that she’s encountered other wannabe scammers seeking money on the platform recently. Indeed, authorities across the country have warned that dating apps are routinely used by swindlers in “pig butchering” scams, which combine a romance hoax and crypto investment scheme.

“They probably were sitting in the same room, just playing me like a fiddle,” Francis said of David and Robert. “They both acted like they hated the other one.”

For months, Francis still believed David was coming to America to be with her, until he asked for another $250,000 to get out of his military contract. When she told him she didn’t have that kind of money, he suggested she obtain a loan against her house to acquire the funds. “When I talked to him and he was willing to let me sell my home, yeah, okay, that’s it. You don’t care about me,” Francis recalled thinking.

“I believed what the guy said, because I guess I wanted to,” Francis says now. “I wanted to hear the bullshit. I wanted to hear the niceness. And I’m just looking at some of the stuff he wrote to me and I was like, ‘Oh, my God, I fell for that. I fell for that hook, line and sinker.’”

Francis says she blocked David, but he kept contacting her via other accounts.

Finally, she confided in her family about what happened, and her daughter sent her information about the online dating investigation service Social Catfish. She decided it was time to ask for help.

Social Catfish is one of several emerging companies dedicated to tracking down sophisticated fraudsters where regular law enforcement cannot. Founded in 2013, the company started by investigating online love matches who daters thought might not be telling the whole truth, or even worse, lying about their identity. (The term “catfish” was popularized by a 2010 documentary about a man who starts dating a woman he met on Facebook who turned out to be faking her identity.) The company added a crypto investigations unit earlier this year, after seeing a “massive uptick” in the number of customers coming to them with crypto-related scams, according to President David McClellan.

To help track down the perpetrators, Social Catfish partners with the Blockchain Intelligence Group, the creators of a proprietary software that both visualizes blockchain data and adds open-source and social media data on top of it. Instead of the endless spreadsheets that Bill Callahan, the director of government and strategic affairs at the group, used to receive in his job as a financial investigator at the DEA, his clients are handed what looks like a flowchart, showing which wallets the crypto was sent to and which it is being held in now.

The software also helps identify whether the money has been sent to an "exchange"—a kind of trading platform for crypto—that law enforcement can subpoena or a private attorney can sue to get the funds back. And it pulls in open-source data, court records, and social media to try to identify the people behind the wallets, or see if they were tied to any other illegal activity.

"Every day our analysts are pulling in and ingesting information off of social media, off of the dark web—wherever illicit intelligence may be," Callahan said. "And then we're pulling in crypto intelligence, and then marrying it up.'

***"I want other women to know that this goes on. You're not above it. You would think that you're smarter than this, because honestly, I thought I was smarter than this."***

Social Catfish and Blockchain Intelligence Group aren't alone in offering crypto sleuthing services. CipherBlade, a "Blockchain Intelligence Agency" with a logo that looks conspicuously like the CIA's, was founded in 2017 by a former soldier named Rich Sanders, after he had some success helping friends who had had their crypto stolen. Now, the firm works on crypto-related crimes from investment fraud to romance scams to kidnappings, and even acts as an expert in civil and criminal cases, according to Sibenik, the lead case

manager. (The largest percentage of their cases are divorces in which a partner thinks their estranged spouse is hiding crypto assets, he added.)

TRM Labs, based in San Francisco, also offers software that helps track cryptocurrency transactions and identify the real people behind the anonymous wallets. Chris Janczewski, the company's head of global investigations, said the group often works with law enforcement, as well as with major exchanges like FTX and Coinbase that want to prevent money laundering on their platforms. (Experts say their experience with other exchanges in this regard varies—some are reluctant to cooperate with investigators, seeing it as a business advantage to let the fraudsters continue to operate unchecked.)

Janczewski, a former IRS special agent, sees his company as occupying the "gray zone" between cases big enough for the FBI or SEC to take over, and smaller ones that local law enforcement can't handle on their own. "That's one of the things that drew me to this position at TRM," Janczewski said, "is that we can kind of help bridge that gap."

But experts warn that gap could expose victims to even more fraud. As Francis learned with "Robert," some of the people claiming to help recover crypto are actually running scams of their own. Jan Santiago, deputy director Global Anti-Scam Organization, which assists victims of romance scams, said many of the sites that turn up in a typical Google search for crypto recovery agencies either outright steal money from their clients, or take money upfront and deliver unsatisfying returns.

The truth is, most experts agree, even with a professional, well-respected crypto investigation company, the chances of getting your stolen funds back are slim.

Francis first contacted Social Catfish via their YouTube channel, "Catfished," where they post weekly videos about cases they helped solve. The team sent her a generic background form to fill out and asked for any pictures or

evidence she had. They also set up a background call with Francis, and, after hearing her story, decided to dive in.

First, the team searched the web for any hints of who the scammers could be. They plugged in the email addresses and phone numbers Francis had used to contact them, hoping that identifying information about them had been leaked in data breaches. (Most people's numbers and email addresses will be the subject of some type of data leak if they use them for long enough.) The search turned up nothing, meaning the scammer had likely created the email account and secured the phone number shortly before contacting Francis.

Then, Social Catfish employed a bit of subterfuge, getting Francis to send David a link to a website that she claimed would send him money via gift cards. (In a bit of foreshadowing the scammer missed, the website was called fyougiftcards.com.) Instead of sending him money, the website scraped David's IP address and sent it to Social Catfish, giving them a vague idea of where in the world he lived: Not North Korea, but Nigeria.

The company also took a record of all of Francis's Bitcoin transfers, asking for the date, time, and wallet address for each transaction. They sent the information to the Blockchain Intelligence Group, which used its software to track the funds through a maze of 20 different wallets to one account on the world's biggest crypto exchange: Binance. They then referred the case over to law enforcement, knowing that they would have the easiest time requesting the stolen funds from the exchange.

But the company's work wasn't quite done. Since Francis had contacted them via their YouTube channel, they staged a viral-video-worthy confrontation between victim and scammer, getting Francis to call David and confront him about his lies on camera.

"David, everything you've ever done and ever said to me was a lie," Francis, then using the pseudonym "Karen," fumed in the footage's expletive-laden confrontation.

“That’s bullshit,” a man with a foreign accent later replied.

The video, “Woman loses $300k; gets engaged to scammer,” has more than 112,000 views.

Francis says she contacted the FBI in California with the new information and for several weeks spoke to a local agent, who ultimately informed her the agency wouldn’t touch any case that didn’t result in at least a $500,000 loss.

She filed a complaint with Nigeria’s Economic and Financial Crimes Commission (EFCC), as well as the FBI’s Internet Crime Complaint Center (IC3) and the FTC. No agency has been able to take on her case.

Laura Eimiller, a spokeswoman for the FBI’s Los Angeles field office, couldn’t comment on Francis’ case but suggested victims file complaints on IC3’s website. She said the agency is unable to investigate every case “from a sheer resources standpoint,” or recover lost funds “particularly if the money is sent out of the country, which is why it is so important to educate the public about these schemes so they can identify the signs and avoid being victimized.”

In an email, the EFCC told The Daily Beast that it received a petition from Francis and that an “investigation is ongoing.” The FTC didn’t return messages.

“You have to lose a half a million dollars before they’ll take your case, even if you’re a little old lady, and they took your life savings,” Francis said. “That to me is not law enforcement. It’s not, I’m sorry. I got a problem with that.”

In the meantime, Francis began to research similar online scams and bonded with others who’d fallen prey to fake suitors on Facebook groups like ScamHaters United.

“I want other women to know that this goes on,” Francis told The Daily Beast. “You're not above it. You would think that you’re smarter than this, because

honestly, I thought I was smarter than this. But guess what? I wasn't. They got me. It doesn't feel good to get gotten."

She's still processing the deceit. "He broke my heart," Francis said. "I was crushed. Devastated, cried, cried so many nights. And for someone I've never even met."

"It's amazing. The heart, when you feel that deeply, it just counteracts the brain completely."

**Kate Briquelet**

Senior Reporter
@kbriqueletkate.briquelet@thedailybeast.com

**Emily Shugerman**

Senior Reporter
@eshugermanEmily.Shugerman@thedailybeast.com