PROFESSIONAL SERVICES

FRAUD HITS HOME

How a Sacramento law firm nearly lost a $500K settlement to wire fraud

A Sacramento law firm nearly lost a $500K settlement to wire fraud. Here's how it happened.

SBJ PHOTO ILLUSTRATION; GETTY IMAGES

By Mengyuan Dong – Data Reporter, Sacramento Business Journal
Feb 8, 2024

Listen to this article 10 min

Officials at Galt Joint Union High School District, former basketball coach Angela DaPrato and their respective attorneys had reason to believe they had reached the end of a three-year ordeal last March, when they had come to a settlement of the lawsuit that DaPrato had filed against the district in 2020.

But it turned out that that wasn't the end of their story.

A scammer, believed to be based in Nigeria, impersonating legal staff and using fraudulent internet domain names, nearly stole the $500,000 settlement payment from the school district's defense counsel.

The ensuing investigation by the Sacramento Valley Hi-Tech Crimes Task Force unveiled more than 50 fraudulent internet domain names targeting institutions in the U.S., including several law firms in the Sacramento region.

Law enforcement ultimately recovered $480,000 of the money in August. But the situation serves as a cautionary tale for business leaders about the growing risk of wire fraud.

"It's a good thing for our community and beyond to get the word out," said Richard Linkert, a partner at Matheny Sears Linkert and Jaime LLP, the firm that suffered the fraud. "Those kinds of potentials are out there, and people just need to be very vigilant."

The four-county Sacramento region saw at least 140 "business email compromise" scams in 2023, resulting in a collective loss of nearly $16 million, according to data from the FBI Internet Crime Complaint Center (IC3). The data also shows that California has been the top state in the U.S. by number of cybercrime victims and victim loss, and the numbers rose each year from 2020 to 2022.

Although methods and narratives the criminals use keep evolving, the roots of wire transfer scams are always getting in the middle of business transactions, separating the parties and intercepting the money, said Nathaniel Le, supervisory special agent at the

FBI's Sacramento field office. Le urges businesses to pay attention to subtle changes when communicating with another party regarding money and data transfer.

"Any business that has and sends money can be a target," Le said.

The settlement originated from a lawsuit filed in May 2020 by DaPrato, who was represented by Telfer Law in Sacramento. Once the head coach of the Galt High School varsity girls basketball team, DaPrato sued the Galt Joint Union High School District, alleging harassment and unequal treatment of herself and her team. Linkert's firm, known as MSLJ, represented the school district.

On March 1, 2023, the parties reached a final version of the settlement offer. The agreement called for the school district to pay $500,000 in two separate checks to DaPrato and Telfer Law.

The same day, Linkert received an email from someone he thought was Telfer Law's paralegal, Skylar Murphy. The email requested a wire transfer of the settlement money instead of a check.

Linkert said he was confused. Still, after several rounds of email communication, Linkert said that he and his client were convinced, believing that Telfer Law was having trouble depositing checks at the time. The wire transfer request was accepted on March 6. About a week later, Linkert had the funds wired through Chase Bank.

Shortly after, his office received a voicemail from Telfer Law's paralegal, stating that they didn't want a wire transfer. Telfer Law attorney Jill Telfer later told the Business Journal that she was eager to contact Linkert because she received an email notification from her bank, U.S. Bank, stating that a wire transfer had been processed and would be posted to her account soon. It's unclear why Telfer was notified by her bank, given that the money was actually wired into the scammer's account.

But soon after the voicemail from Telfer's office, Linkert said he received an email saying, "please disregard the voice message."

When MSLJ hit 'panic time'

On March 21, Linkert attempted to schedule a meeting with Telfer Law to wrap up the settlement. But soon after, he got a response from Telfer. That email mentioned the checks again — "Once the check comes in and clears, we will file a dismissal."

"That's when the light bulb went off," Linkert said.

Soon after communicating about the conflicting emails, the firms both realized an internet scam had occurred.

"It became a panic time here," Linkert said. "Half a million dollars of our client's money is gone."

The scammer had not only impersonated Telfer Law's paralegal to ask for the wire transfer. They were communicating to Telfer Law in the meantime, placating the firm that the money would come soon. They also obtained Telfer Law's and DaPrato's W-9 tax forms for the transfer.

To trick the parties, the scammer created false domain names on internet domain registry GoDaddy. These fake domain names were visually similar to real ones — using telferlavv.com instead of telferlaw.com; and rnathenysear.com instead of mathenysears.com.

Telfer told the Business Journal that she had known attorneys at MSLJ for years, and had even worked for the firm before starting on her own.

The scammers "mimic the way of how we communicate, like word choice and stuff," Telfer said.

"They are very sophisticated," said Detective Justin Varner, who was appointed by the Sacramento County Sheriff's Office's Hi-Tech Crimes Task to investigate the case. "I think they read a lot of emails trying to figure out who they were impersonating to make it seem as realistic as possible, so they could get the maximum amount of the money."

Advised by a retired FBI special agent, MSLJ first filed a report of the fraud to the IC3. They also went to Chase Bank to report the fraud and freeze the school district's bank account.

Varner was appointed to investigate the case after MSLJ called the police. He got the information for the bank account the wire transfer went into, obtained a search warrant for the account holder's information, and then traced down the suspected scammer.

His investigation found that the suspected thief's IP address, cellphone number and Google account traced to Nigeria.

However, the actual name of the scammer couldn't be identified. It turned out that the bank account they used wasn't theirs; it belonged to a Texas woman who was the victim of a separate romance scam the suspected thief had allegedly initiated.

Whether and how the scammer had obtained previous communications between the law firms couldn't be determined. Varner said it's possible that a previous phishing email might have induced law firm staff to click on a link that gave the scammers access to the targets' email accounts.

Linkert said his firm goes through a security analysis with insurance companies every year to make sure its systems are safe and protected. Telfer said she hired a computer forensic expert to investigate if her firm had been hacked. The results indicated no intrusion or data breach.

Le said scammers are likely to familiarize themselves with their targets as much as they can, such as by reading public documents from lawsuits and familiarizing themselves with the facts, before instigating their scams.

"Scammers always do their homework," Le said.

According to the FBI, business email compromise scams are one of the most financially damaging cybercrimes. They involve tricking individuals or institutions into sending money or sensitive data to fraudulent accounts, usually appearing to come form a known source making a legitimate request. The IC3's 2022 Report shows that business email compromise is the third-largest class of cybercrime in California, after investment scams and cryptocurrency scams, in terms of the amount of money lost to victims. Victim losses from business email compromise scams in the state totaled $439 million in 2022, an 8% increase from 2021 and double the amount from two years earlier.

Looking at the Sacramento region specifically, a total of 72 business email compromise scams were reported to the FBI last year in Sacramento County, 42 in Placer, 18 in Yolo and eight in El Dorado. Victims in Placer County lost more than $10 million, or half of the four-county total.

The incident led to Telfer Law filing a motion to enforce the settlement on May 10, more than a month after the initial payment deadline. Telfer said she understood the situation and tried to offer help, but she was dissatisfied with the lack of communication from the other side when she was requesting updates on the situation.

"That's the takeaway — if this happens to anybody, you need to pick up the phone and talk to your opposing counsel," Telfer said.

Given it was a wire transfer, the issuing bank had to send a letter of request to the suspect bank to get the money back, Varner said. He said his search warrant results came in between May and August, and the money was returned in August 2023.

In the end, $480,000 of the wired money was clawed back. The rest had been used to purchase bitcoin and couldn't be recovered.

How to take precautions against fraud

Varner's investigation also revealed about 52 other fraudulent domain names purchased by the same suspected individual or group. He was able to warn 28 possible real businesses.

This endeavor saved a Folsom law firm that was just about to wire more than $900,000 to the scammer's account, Varner said.

The FBI only gets involved in cybercrime cases if the loss is over $1 million. However, Le still urges businesses to report their case to IC3, regardless of the amount of the loss, within 72 hours. Most often, scammers victimize many people, he said, and the FBI reads all the cases, big or small, to connect the dots and paint a full picture of the crime.

Le said that using different forms of communication can help to avoid fraud — maybe initiating a phone call if the previous correspondence was by email, ideally to a different contact as well.

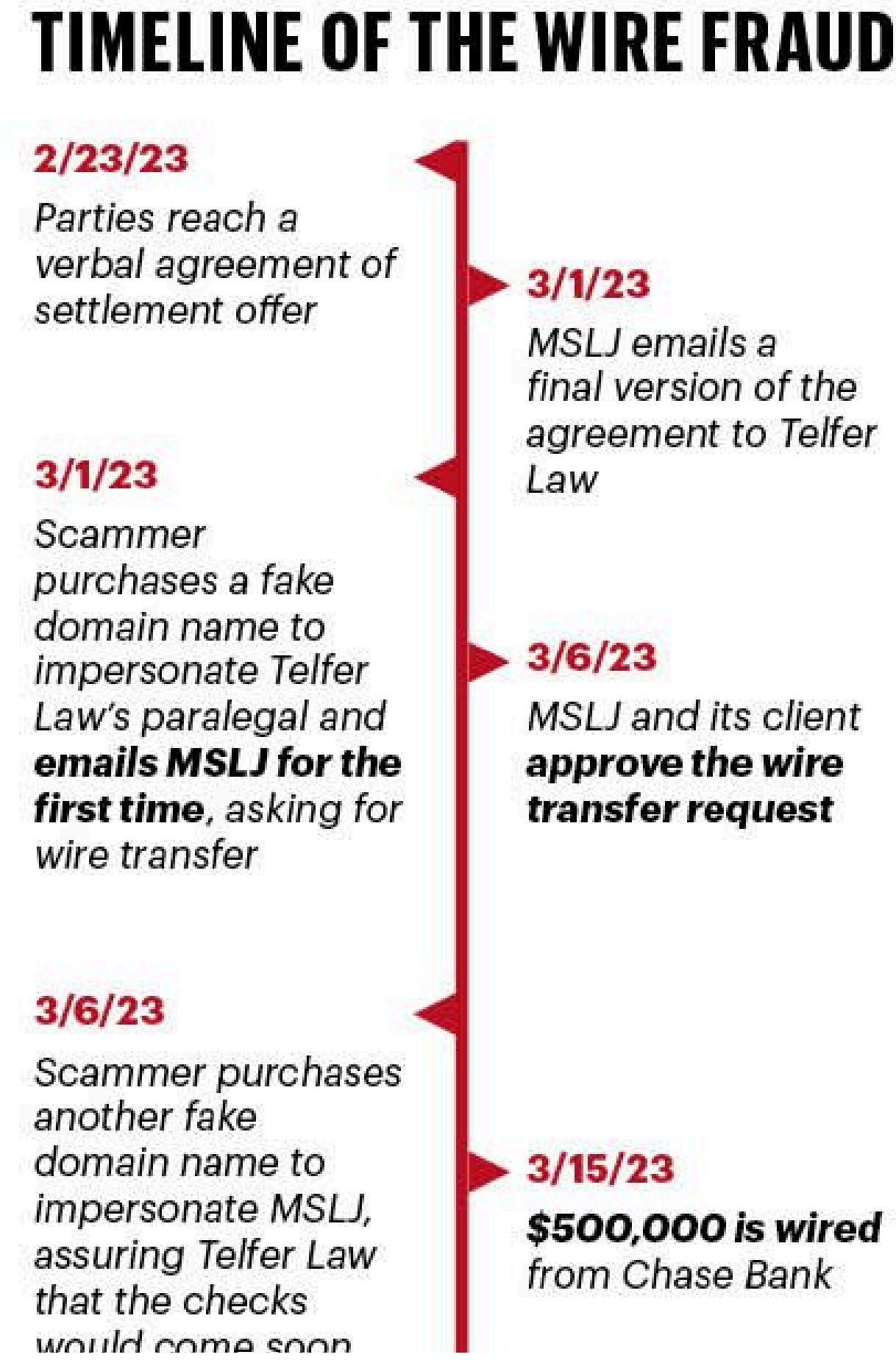
Le said it's also crucial to be prepared mentally for the possibility of fraud.

"In the online world, anybody can be anybody," he said. "I would promote the precautionary mindset when it comes to moving money and transferring data."

In a seminar Telfer gave to the plaintiff's bar in San Francisco last year, she suggested her fellow attorneys take the following steps if they are a victim of wire fraud: retain a forensic expert, contact the U.S. Attorney's Office and a malpractice insurance carrier, reach out to law enforcement and file a motion to enforce settlement.

MSLJ and Varner also presented at the Association of Defense Counsel of Northern California and Nevada's annual event about the incident in December.

"I've settled more than $100 million of cases in the last six months, and I'm not doing wire transfers anymore," Linkert said. "I don't want to have anything to do with it."


TIMELINE OF THE WIRE FRAUD
2/23/23
Parties reach a verbal agreement of settlement offer
3/1/23
MSLJ emails a final version of the agreement to Telfer Law
3/1/23
Scammer purchases a fake domain name to impersonate Telfer Law's paralegal and emails MSLJ for the first time, asking for wire transfer
3/6/23
MSLJ and its client approve the wire transfer request
3/6/23
Scammer purchases another fake domain name to impersonate MSLJ, assuring Telfer Law that the checks would come soon
3/15/23
$500,000 is wired from Chase Bank

would come soon

3/15/23

Telfer Law receives a wire transfer notification, texted and left a voicemail to MSLJ, asking for clarification

3/15/23

Scammer emails MSLJ soon after, confirming they have received the funds and telling the firm to disregard the voicemail

3/21/23

MSLJ emails Telfer Law's attorney to finalize the settlement

3/21/23

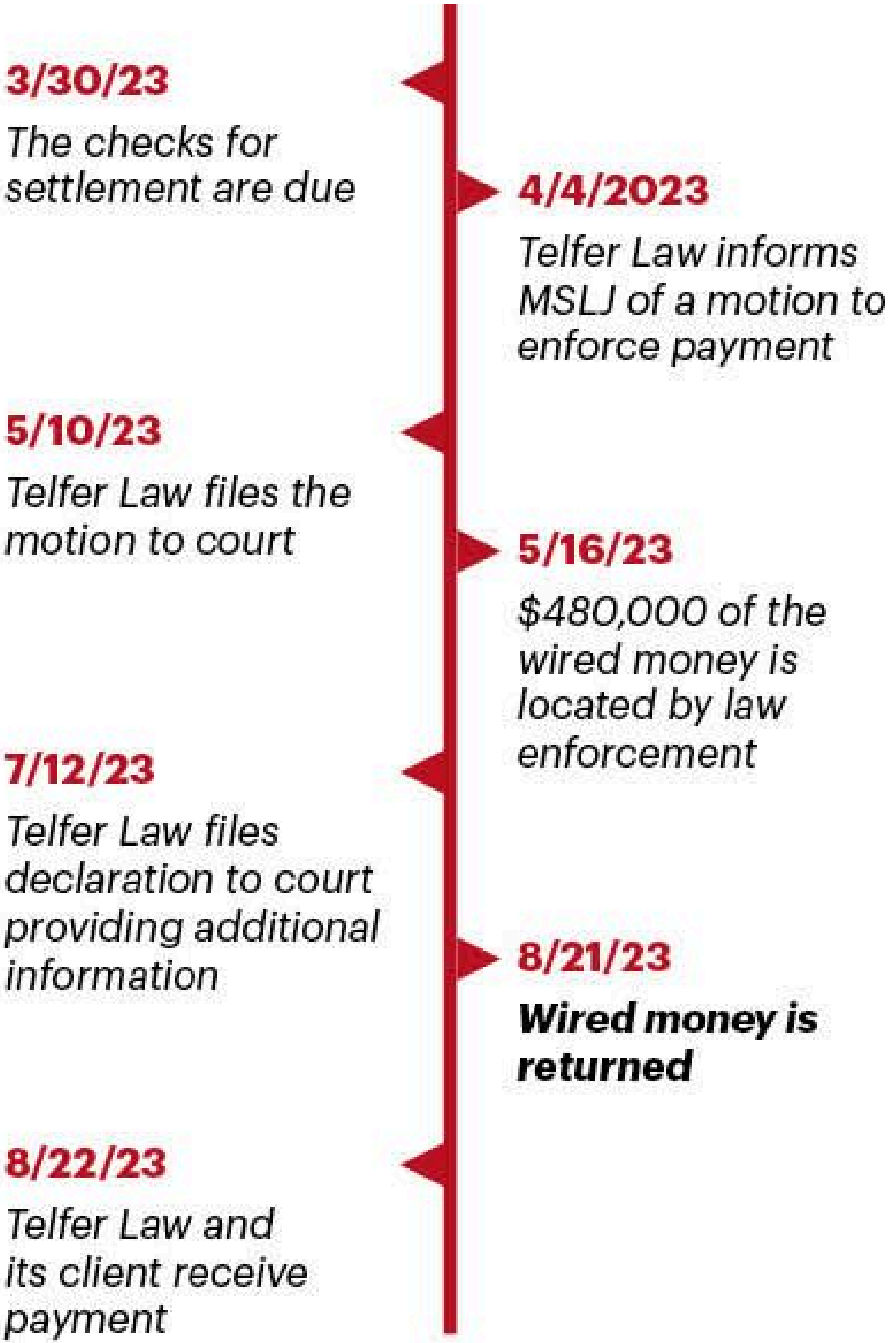
Telfer replies that they are still waiting for the checks

3/21/23

***The scam is revealed**. MSLJ contacts law enforcement*

3/22/23

MSLJ goes to Chase to freeze client's bank account


3/30/23
The checks for settlement are due
4/4/2023
Telfer Law informs MSLJ of a motion to enforce payment
5/10/23
Telfer Law files the motion to court
5/16/23
$480,000 of the wired money is located by law enforcement
7/12/23
Telfer Law files declaration to court providing additional information
8/21/23
Wired money is returned
8/22/23
Telfer Law and its client receive payment