Losing $450,000 in Three Days: Hackers Trick Victims Into Big Wire Transfers

By Rachel Louise Ensign

In 2018, Frank Krasovec took on a $1 million personal line of credit from PlainsCapital Bank. A few months later, he went on a business trip. When he returned, $450,000 was missing.

Mr. Krasovec, the chairman of Dash Brands Ltd., which owns Domino's Pizza Inc. DPZ -0.32% franchises in China, said he soon learned that someone had hijacked his email and asked his assistant to wire the money to a Hong Kong account.

Fraudsters are stealing billions of dollars each year through this type of scam, which combines sophisticated hacking with wire transfers, an old-fashioned but efficient way to move money overseas. Banks and law-enforcement officials are struggling to curb the problem, while victims like Mr. Krasovec say they are finding it nearly impossible to get their money back.

Years ago, lenders only had to worry about real-life bank robbers. Now, the wire-transfer scam puts them in a tough position. Customers expect them to move money quickly for legitimate transactions, while also guarding against hackers that have infiltrated clients.

The largest banks are most likely to be conduits for the wire-transfer scams, according to the American Bankers Association. But community banks, with much smaller technology budgets to build their defenses, are also vulnerable.

The Federal Bureau of Investigation received reports of nearly $1.8 billion in losses from this type of scam in 2019, up from about $1.3 billion the prior year. The agency estimates total losses world-wide, which include those not reported to the agency, were $26 billion between June 2016 and July 2019. The transfers primarily go to banks in Hong Kong and mainland China, where chances of recovering the money are slim, the agency said.

Victims include "the elderly, college students, nonprofits, religious organizations, celebrities, CEOs of companies," FBI Supervisory Special Agent Zacharia Baldwin said in an interview. "It could be anybody."

Hackers can break into a target's email by trying out passwords made public in previous data breaches. They also may use phishing schemes like those used against political campaigns and in corporate espionage. The hackers then commandeer an account and impersonate the victim, asking assistants or colleagues to initiate a wire transfer.

Mr. Krasovec, 76 years old, isn't sure how his email was compromised. He said he believes the fraudsters, once inside his servers, tracked his travel plans and waited until he was out of the office to message his assistant.

"Carol…please wire $150,000," the hackers wrote Mr. Krasovec's assistant from his email account, the executive said. It was around 11:30 p.m. in Shanghai, where Mr. Krasovec had landed hours earlier and was fast asleep, he said.

Unlike cruder scams that might ask for money in broken English, the note sounded just like him. An attachment with transfer instructions showed intimate knowledge of his accounts, he said.

The assistant asked PlainsCapital Bank to wire the money. The Dallas-based community bank had courted Mr. Krasovec's business for months, he said, after poaching his longtime banker at Wells Fargo & Co.

PlainsCapital called his assistant to confirm the request, then made the transfer. The bank declined to comment.

Mr. Krasovec believes the fraudsters, once inside his servers, tracked his travel plans and waited until he was out of the office to message his assistant.

Photo of Frank Krasovec: Brent Humphreys for The Wall Street Journal

Meanwhile, in China, Mr. Krasovec powered through 14-hour workdays unaware anything was amiss. The pizza chain has grown quickly there after switching to a local menu that includes seafood toppings.

Three days after the first transfer, at 10:26 p.m. local time, intruders asked Mr. Krasovec's assistant to wire another $300,000, according to Mr. Krasovec. The hackers had changed Mr. Krasovec's email settings so their correspondence was quickly deleted, according to Kyle Camp, a technology consultant who examined the hack for Mr. Krasovec.

A few days later, Mr. Krasovec flew home to Austin. Catching up in their offices overlooking Lady Bird Lake, his assistant mentioned she "took care of the wires."

"What wires?" he recalls saying.

When she explained, he said he began to feel "absolutely sick."

He frantically called his banker at PlainsCapital Bank, who said there was nothing the bank could do. Mr. Krasovec said the bank then stopped returning his calls.

He is now suing PlainsCapital, saying he shouldn't have to repay the stolen money because the bank failed to put proper antifraud controls in place.

PlainsCapital Bank said in a court filing that the loss was "undoubtedly the fault of [Mr. Krasovec's] own failure to implement appropriate internal controls to prevent his company and its employees from falling victim to a third-party scam." The bank said in filings that Mr. Krasovec must repay the money with interest.

The case is continuing in the Texas court system.

Under decades-old consumer-protection laws, consumers are often entitled to refunds of unauthorized charges. But that generally doesn't apply to wire transfers requested after a customer was tricked by hackers, according to the American Bankers Association.

Sometimes, consumers who catch the fraudulent wires can halt them by immediately calling their bank, said Don Vilfer, an investigator who works on these cases. But that isn't certain: One law firm called Bank of America Corp. BAC -1.41% about an hour after a fraudulent request, but still lost $500,000, according to court documents. Bank of America declined to comment.

Some banks try to prevent fraud by calling the customer to confirm large wire-transfer requests. Mr. Krasovec said PlainsCapital Bank should have called him, not just his assistant. The bank declined to comment beyond its court filings.

Mr. Krasovec has put in place tougher passwords and two-factor authentication, said Mr. Camp, the technology consultant. Legal costs have added $300,000 to his already-sizable loss, and he is concerned about his reputation.

"It makes me look like a dummy," he said of the fraud.