



## **N.Y. Firm Faces Bankruptcy from \$164,000 E-Banking Loss**

A New York marketing firm that as recently as two weeks ago was preparing to be acquired now is facing bankruptcy from a computer virus infection that cost the company more than \$164,000.

Karen McCarthy, owner of Merrick, N.Y. based Little & King LLC, a small promotions company, discovered on Monday, Feb. 15 that her firm's bank account had been emptied the previous Friday. McCarthy said she immediately called her bank – Cherry Hill, N.J. based TD Bank – and learned that between Feb. 10 and Feb. 12, unknown thieves had made five wire transfers out of the account to two individuals and two companies with whom the McCarthys had never had any prior business.

“She was told to go to the branch next day, and she did, and the people at the branch were very nice, apologetic, and said, ‘Whatever happened, we’ll replace it,’” Karen McCarthy’s husband Craig said. “She called them up on Wednesday, and they gave her the runaround. Then she finally got to talk to someone and they said ‘We don’t see the error on our side.’”

Immediately before the fraud occurred, Mrs. McCarthy found that her Windows PC would no longer boot, and that the computer complained it could not find vital operating system files. “She was using it one day and then this blue screen of death just came on her screen,” said a longtime friend who was helping McCarthy triage her computer.

Later, McCarthy’s friend would confirm that her system had been infected with the ZeuS Trojan, a potent family of malware that steals passwords and lets cyber thieves control the infected host from afar. ZeuS also includes a feature called “kill operating system,” which criminals have used in prior bank heists to effectively keep the victim offline and buy themselves time to make off with the cash.

Karen McCarthy said TDBank has dug in its heels and is now saying it has no responsibility for the loss.

“I had a company that was interested in purchasing us, but they’re not going to do that now. I’m basically looking at bankruptcy, because I have very little money to operate on now.”

“They feel that because [the thieves] compromised my computer that it’s my responsibility and that I should look into my insurance, but I don’t have insurance,” McCarthy said. “I had a company that was interested in purchasing us, but they’re not going to do that now. I’m basically looking at bankruptcy, because I have very little money to operate on now.”

Krebs on Security spoke briefly with John G. McCluskey, vice president of TDBank’s corporate security and investigations. McCluskey referred all questions about the incident to the bank’s marketing department, which hasn’t returned calls seeking additional information and comment.

As Mrs. McCarthy found out the hard way, businesses do not enjoy the same protections that consumers have against online banking fraud. Most banks will work with commercial customers to try and reverse any fraudulent transfers, but the chances of that succeeding diminish rapidly after the first 24 hours following unauthorized activity. What's more, banks are under no obligation to reimburse commercial customers victimized by cyber fraud.

McCarthy said she never would have done online banking for her business if she had understood how precarious it was for her business.

"I go to the bank and I see everywhere signs that your money is insured up to \$250,000, but maybe they should have a little asterisk next to that saying 'except for businesses,'" she said. "If I had understood that, I wouldn't have been banking online."

McCarthy said a \$41,240 wire was sent to a company in New York called Asbury PHH; two wires totaling nearly \$80,000 were sent to a man in North Carolina; and a \$28,640 wire was sent to a Kimto LLC in California. Efforts to track down any individuals tied to those entities were unsuccessful.

The fifth wire was sent to a 59-year-old Kennesaw, Ga. resident named Pamela Biagi, who said she got the money after signing up for a work-at-home job over the Internet. Biagi said her employer called itself Adams Interiors, and used the Web site name interiors-a.com (that site is no longer online).

As it happened, that Web site essentially hijacked the good reputation of an interior design firm in Brooklyn, N.Y., claiming it was one and the same and pointing to the firm's stellar reputation with the Better Business Bureau. Biagi said this was part of the reason she felt good about accepting the job offer.

"I did an online and phone interview with them. They wanted to hire me to be a financial agent, and to help their subcontractors who were going around the country doing interior design work," Biagi said.

Then, on Feb. 12, she received a wire transfer of \$14,875 with instructions to wire the money to another individual in Georgia. Suspecting fraud, Biagi's bank promptly froze her account.

"The guy I was supposed to send the money to kept calling me...he was real nervous and kept asking me if I'd sent the money," Biagi recalled in a phone conversation with krebsonsecurity.com. "I told him, 'No, I'm sitting here with police officers and people from the bank because of all this.'"

When confronted with the news of where the money had come from, Biagi said she was "horrified."

"This has been an absolutely horrible experience for me, and I feel terrible for [Little & King]," she said. "I'm really glad they stopped it when they did. To think that I have been participating in something so horrendous like this is awful. It's a black mark on my soul."