April 19, 2011

3 banks stung by elaborate wire fraud

By ADAM BELZ
abelz@dmreg.com

The bad guys don't need guns and getaway cars any more.

Three Iowa financial institutions have lost $2 million in a series of fraudulent transfers to Hong Kong in recent months. The thieves likely used a combination of email and telephone calls to pull off the heists, highlighting the growing sophistication and reach of criminals intent on stealing from banks.

Thieves impersonating customers called and requested wire transfers, each of them about $500,000, according to an internal memo at Bankers Trust based on information provided by law enforcement. The memo did not name the victimized banks but made clear Bankers Trust - the victim of an online theft last year - was not one of them.

One of the three was MetaBank, a Storm Lake-based subsidiary of a publicly traded company that disclosed the $1.1 million loss to shareholders in December. MetaBank released a statement saying it is cooperating extensively with law enforcement. The other banks remain unidentified.

The thieves - who experts say could be anywhere in the world - somehow forwarded wealthy customers' phone numbers to disposable cellphones, and had enough information about the customers to answer sensitive questions in follow-up calls, according to the memo.

"They're smarter and smarter and smarter," said Jodi Paardekooper, Bankers Trust's security officer, who wrote the memo. "There's a whole underground world that we can't even comprehend."

Such crime is growing in frequency, experts say, though banks anxious to maintain their reputations for security rarely let on when it occurs. The FBI is investigating

but declined to release any information. Representatives of the Iowa Division of Banking and Iowa Bankers Association said they knew nothing about the probe.

"This particular kind of thing is very important for people to know about, and it doesn't get reported," said Avivah Litan, an analyst at Gartner Inc., an information technology research and advisory firm. "It's definitely happening."

Consumers don't lose their money in cases like the recent ones in Iowa. The bank either tracks the money down, gets its insurance company to cover it or takes the loss, said Vaughn Noring, bank bureau chief for the Iowa Division of Banking.

Overseas transfers wouldn't necessarily raise a red flag in Des Moines because of the amount of international business conducted here, Noring said. Also, wealthy bank clients are more likely to make international transfers.

Banks verify that a customer approves of a transfer by calling him or her back at the phone number the bank has on file, Noring said. The callback usually includes a series of security questions only the customer should be able to answer.

Thieves are starting to get around this, said Litan, the analyst at Gartner.

"They're beating all these methods," she said.

Litan has no direct knowledge of the cases in Iowa, but said such thefts are generally a three-pronged attack.

The criminals identify a wealthy bank customer's account. They send the customer a targeted, convincing-looking email with an attachment that, when opened, downloads software onto the customer's computer.

When the customer types the bank's name into an Internet browser, the software records the customer's keystrokes, Litan said, giving the criminals their username and password.

Meanwhile, the criminals send a similar email to an employee at one of the companies that stores the customer's security questions and answers - credit reporting agencies, debt collectors. The thieves then know the answers to security questions banks use to verify the customer's identity.

"What's increasing is the use of these techniques not just against bank accounts, but against businesses, intellectual property," Litan said.

The final piece is a phone call to the customer's telephone company. The perpetrator, impersonating the customer, tells a customer service representative that his phone is dead and that all calls should be forwarded to a different number. Telephone company security measures are relatively straightforward - date of birth, last four digits of a Social Security number - and it's easy for the criminal to get the calls forwarded, Litan said.

Then, for the thieves, it's simple. They call the bank to request a wire transfer, answer questions to which they already have a list of answers, and poof: $500,000 has left Des Moines, landed in Hong Kong, and moved on from there to who knows where.

"Email and the electronic age has just made these things much easier for the thieves to pull off," Noring said. "Now they can be living in a country on the other side of the globe and steal from you."

The thefts are not the first case of a breach in bank security in Iowa. More than $600,000 was stolen electronically from a Bankers Trust account belonging to the Catholic Diocese of Des Moines in August.