Hackers stole $45 million in bank card breach (Update)

9 May 2013, by Colleen Long

This Feb. 19, 2013 surveillance image released by the U.S. Attorney's Office in New York City shows a man referred to as "defendant Reyes" allegedly using fraudulent magnetic cards to steal money from one of several cash machines in Manhattan. Federal prosecutors on Thursday, May 9, 2013, said that a gang of cyber-criminals stole $45 million in a matter of hours by hacking their way into a database of prepaid debit cards and then draining cash machines around the globe. (AP Photo/U.S. Attorney's Office)

A worldwide gang of criminals stole $45 million in a matter of hours by hacking their way into a database of prepaid debit cards and then draining cash machines around the globe, federal prosecutors said—and outmoded U.S. card technology may be partly to blame.

Seven people were under arrest Thursday in the U.S. in connection with the case, which prosecutors said involved thousands of thefts from ATMs using bogus magnetic swipe cards carrying information from Middle Eastern banks. The fraudsters moved with astounding speed to loot financial institutions around the world, working in cells including one in New York, Brooklyn U.S. Attorney Loretta Lynch said.

She called it "a massive 21st-century bank heist" carried out by brazen thieves.

One of the suspects was caught on surveillance cameras, his backpack increasingly loaded down with cash, authorities said. Others took photos of themselves with giant wads of bills as they made their way up and down Manhattan.

Here's how it worked:

Hackers got into bank databases, eliminated withdrawal limits on pre-paid debit cards and created access codes. Others loaded that data onto any plastic card with a magnetic stripe—an old hotel key card or an expired credit card worked fine as long as it carried the account data and correct access codes.

A network of operatives then fanned out to rapidly withdraw money in multiple cities, authorities said. The cells would take a cut of the money, then launder it through expensive purchases or ship it wholesale to the global ringleaders. Lynch didn't say where they were located.

It appears no individuals lost money. The thieves plundered funds held by the banks that back up prepaid credit cards, not individual or business accounts, Lynch said.

She called it a "virtual criminal flash mob," and a security analyst said it was the biggest ATM fraud case she had heard of.

There were two separate attacks, one in December that reaped $5 million worldwide and one in February that snared about $40 million in 10 hours with about 36,000 transactions. The scheme involved attacks on two banks, Rakbank in the United Arab Emirates and the Bank of Muscat in Oman, prosecutors said.

In this Saturday, Jan. 5, 2013 file photo, a person inserts a debit card into an ATM machine in Pittsburgh. A gang of cyber-criminals stole $45 million in a matter of hours by hacking their way into a database of prepaid debit cards and then draining cash machines around the globe, federal prosecutors said Thursday, May 9, 2013. (AP Photo/Gene J. Puskar, File)

This Feb. 19, 2013 surveillance image taken from a graphic released by the U.S. Attorney's Office in New York City shows a man identified as "defendant Reyes" allegedly using fraudulent magnetic cards to steal money from one of several cash machines in Manhattan. Federal prosecutors on Thursday, May 9, 2013, said that a gang of cyber-criminals stole $45 million in a matter of hours by hacking their way into a database of prepaid debit cards and then draining cash machines around the globe. (AP Photo/U.S. Attorney's Office)

The plundered ATMs were in Japan, Russia, Romania, Egypt, Colombia, Britain, Sri Lanka, Canada and several other countries, and law enforcement agencies from more than a dozen nations were involved in the investigation, U.S. prosecutors said.

The accused ringleader in the U.S. cell, Alberto Yusi Lajud-Pena, was reportedly killed in the Dominican Republic late last month, prosecutors said. More investigations continue and other arrests have been made in other countries, but prosecutors did not have details.

An indictment unsealed Thursday accused Lajud-Pena and the other seven New York suspects of withdrawing $2.8 million in cash from hacked accounts in less than a day.

Such ATM fraud schemes are not uncommon, but the $45 million stolen in this one was at least double the amount involved in previously known cases, said Avivah Litan, an analyst who covers security issues for Gartner Inc.

Middle Eastern banks and payment processors are "a bit behind" on security and screening technologies that are supposed to prevent this kind of fraud, but it happens around the world, she said.

"It's a really easy way to turn digits into cash," Litan said.

Some of the fault lies with the ubiquitous magnetic strips on the back of the cards. The rest of the world has largely abandoned cards with magnetic strips in favor of ones with built-in chips that are nearly impossible to copy. But because U.S. banks and merchants have stuck to cards with magnetic strips, they are still accepted around the world.

Lynch would not say who masterminded the attacks globally, who the hackers are or where they were located, citing an ongoing investigation.

In this undated photo provided by the United States Attorney's Office for the Southern District of New York, Elvis Rafael Rodriguez, left, and Emir Yasser Yeje, pose with bundles of cash allegedly stolen using bogus magnetic swipe cards at cash machines throughout New York. Prosecutors in New York on Thursday, May 9, 2103 said that they are members of worldwide gang of criminals who stole $45 million in hours by hacking into a database of prepaid debit cards and draining cash machines around the globe. An indictment unsealed Thursday accused U.S. cell ringleader Alberto Yusi Lajud-Pena and seven other New York suspects of withdrawing $2.8 million in cash from hacked accounts in less than a day. (AP Photos/U.S. Attorney's Office for the Southern District of New York)

The New York suspects were U.S. citizens originally from the Dominican Republic, lived in the New York City suburb orf Yonkers and were mostly in their 20s. Lynch said they all knew one another and were recruited together, as were cells in other countries. They were charged with conspiracy and money laundering. If convicted, they face 10 years in prison.

Arrests began in March.

Lajud-Pena was found dead with a suitcase full of about $100,000 in cash, and the investigation into his death is continuing separately. Dominican officials said they arrested a man in the killing who said it was a botched robbery, and two other suspects were on the lam.

The first federal study of ATM fraud was 30 years ago, when the use of computers in the financial community was growing rapidly. At the time, the Bureau of Justice Statistics found nationwide ATM bank loss from fraud ranged from $70 and $100 million a year.

By 2008, that had risen to about $1 billion a year, said Ken Pickering, who works in security intelligence at CORE Security, a white-hat hacking firm that offers security to businesses.

He said he expects news of the latest ring to inspire other criminals.

"Once you see a large attack like this, that they made off with $45 million, that's going to wake up the cybercrime community," he said.

"Ripping off cash, you don't get that back," he said. "There are suitcases full of cash floating around now, and that's just gone."