# FBI Warns of Impending Multimillion Dollar Global ATM Cashout, $13.5 Million Taken Already

**Anton Janik, Jr.**
ajanik@mwlaw.com
(501) 688.8888

08/16/2018

According to a confidential FBI alert reported upon by Krebs on Security last Friday, the FBI issued an alert to banks concerning what is called an Unlimited ATM Cashout, attacks of which are expected in the near future. Indeed, shortly after that notice was issued, it came to light that The Cosmos Co-op Bank, LTD (Cosmos Bank) in India had been breached from August 11th through 13th, and thieves were able to steal $13.5 million dollars through ATM Cashouts. There is no indication that the attacks are over, so by all accounts your bank and payment processing clients need to quickly review their security controls.

In an Unlimited ATM Cashout, hackers gain access to a bank or payment card processor, usually through phishing or hacking. Once inside, the hackers remove fraud controls, for example eliminating maximum ATM withdrawal amounts, ATM PINs, and limitations on the number of ATM transactions a given account may have in a day. In addition, hackers may increase account balances to make additional funds available for the next step, including making an unlimited amount of money available. That is the reason this is termed an Unlimited ATM Cashout. (In the standard ATM Cashout, the hackers copy card data but are limited by the withdrawal caps in force on those accounts. In a 2016 attack against South Africa's Standard Bank, thieves withdrew $20 million over two hours, but had to do so by making *14,000* individual transactions.)

Once account balances have been boosted and restrictions on withdrawal have been removed, the hackers create fraudulent copies of otherwise legitimate ATM cards, which data is sent throughout the world wherever branches/payment networks reach—and coconspirators sit. The ATM magnetic stripe information is imprinted on blank cards and at a predetermined time, the hackers all make withdrawals from the ATMs.

Recent incidents include the above Cosmos Bank attack earlier this week, in which ATMs were accessed in Canada, Hong Kong, and India. But don't let that trick you into complacency for clients here in the United States. In May 2016 an employee at The National Bank of Blacksburg (VA) was phished, and hackers disabled anti-theft and anti-fraud protections like 4-digit PINs and daily withdraw limits. In ATM Cashouts conducted against Blacksburg accounts in May 2016 and January 2017, hackers reportedly made away with $2.4 million.

Krebs reports that the ATM Cashout side of the hacks have historically been conducted on Saturdays after banks close or on holidays. In the United States, Labor Day begins in just two weeks, and banks will be closed for at least two days over that holiday. Here's what the FBI advises to help secure your bank and payment processor assets:

- Review your security procedures, including your password requirements, and enable multi-factor authentication using a physical token or device where possible;
- Implement separate duties or dual authentication procedures for account balance or withdrawal increases above a specific level (and check to see if such limitations are currently running and in effect across all of your accounts);
- Implement application whitelisting to block execution of malware on bank systems;
- Monitor, audit, and limit administrator and business critical accounts with the authority to modify account attributes like account balance or withdrawal limits;
- Monitor for the presence of remote network protocols and administrative tools used to conduct post-attack exploitation of the bank network, such as Powershell, Cobalt Strike, and TeamViewer;
- Monitor for encrypted traffic (SSL or TLS) traveling over nonstandard ports; and
- Monitor for network traffic going to geographical regions where you would not expect to see outbound connections from the bank or payment processor.

In addition, you should recheck and reconfirm which users are authorized for elevated rights to your networks, for example those having administrative rights. Look for new domain accounts that don't correspond to actual employees. Check your network and access logs for unusual activity during non-banking hours. In performing this review, you may need to go back several months.

With the urgency of this FBI alert, and knowing the prior patterning of similar attacks occurring on weekends and holidays, your time to prepare and to react to a coming attack may be short. Be on extra alert during the upcoming Labor Day holiday.