New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
JULY 31, 2015

INTERNATIONAL CRIMINAL LAW AND ENFORCEMENT

Expert Analysis

'Unlimited Operations': A New Financial Cyber Threat

By **Nicholas M. De Feis**

By **Philip C. Patterson**

In our last column, we wrote about dangers posed to corporations and law firms by cyber attacks from hackers who secretly take control of host computers.[1] In this column, we describe "Unlimited Operations," a narrower but no less insidious form of cyber attack that poses a particular threat to financial institutions. In a typical unlimited operation, hackers remove security features from bank accounts, increase balances, and then provide teams of "cashing crews" with account information that allows them to make mass ATM withdrawals from the compromised accounts. The lack of security features and increased account balances allow the cashing crews to withdraw money from ATM branches all over the world in amounts far greater than typical withdrawal limits.

While the dangers are especially acute for international banks, the technology could also apply to any corporation that issues any form of credit or debit card—even gift cards. These attacks also use payment processors and vendors as a means to access the card issuer, thus creating potential liability and litigation risk for a variety of corporations.

Our last column described the FBI's most-wanted cyber criminal, Evgeniy Bogachev, who is wanted for orchestrating cyber attacks that are believed to have caused hundreds of millions of dollars in damages. Bogachev is still at large, but the FBI's second most wanted cyber criminal has not been as elusive. On June 24, 2015, the U.S. Attorney's Office for the Eastern District of New York announced the extradition and unsealing of an indictment against Ercan Findikoglu, who is charged with orchestrating a cyber attack that allegedly succeeded in stealing $55 million from a number of banks.[2] The methods purportedly used by Findikoglu and a diffuse network of conspirators pose a threat to banks and a variety of other corporations.

All You Can Eat for Free

The cyber attack allegedly organized by Findikoglu is known as an "unlimited operation" because it involves removing the limits on ATM withdrawal amounts and increasing account balances, and then making massive amounts of fraudulent withdrawals. Findikoglu and alleged co-conspirators whose names remain sealed are accused of orchestrating a world-wide scheme to make countless fraudulent ATM withdrawals from 2010 to 2013.[3] According to the Indictment, beginning in January 2010 Findikoglu and his conspirators hacked into the computer networks of at least three payment processors located in the United States and India. The hackers then focused on MasterCard and Visa prepaid debit cards serviced by the processors, breached the protections setting limits on withdrawals, and dramatically increased the balances in the accounts. They also acquired PIN numbers for the accounts.

The hackers then allegedly distributed the hacked prepaid debit card numbers to a diffuse network of "cashing crews" located throughout the world. The cashing crews encoded the information onto any card with a magnetic stripe, such as gift cards or even hotel room keycards. Once the organizers distributed the PIN numbers for the cards, the cashing crews quickly began making thousands of withdrawals from the accounts. Removing the limits on withdrawals and increasing the balances permitted crews to make hundreds of withdrawals in a matter of hours from only a single account.

Although the banks apparently caught onto the cashouts relatively quickly, the damage had already been done. Over one two-day period, cashing crews operating in 24 countries made 36,000 withdrawals for a total of $40 million. Throughout all of these cashouts, Findikoglu and his conspirators allegedly monitored the transactions and received payments from the crews either electronically or by personal deliveries of hard currency.

The investigation has been carried out by the U.S. Attorney's Office, the U.S. Secret Service, U.S. Immigration and Customs Enforcement, and U.S. Homeland Security Investigations. The charges against Findikoglu include computer intrusion (18 U.S.C. §1030), wire fraud (18 U.S.C. 1343), bank fraud (18 U.S.C. §1344), access device fraud (18 U.S.C. §1029), money laundering (18 U.S.C. §1956) and forfeiture allegations. He has also been charged with obstruction of justice (18 U.S.C. §1512) for allegedly directing conspirators to destroy electronic evidence after a member of a cashing crew was arrested in New York.

Findikoglu is a Turkish national who was arrested in Germany and extradited to the

NICHOLAS M. DE FEIS, *a former federal prosecutor, is a partner at De Feis O'Connell & Rose.* PHILIP C. PATTERSON *is counsel to the firm.*

United States after a series of appeals in German courts. His prosecution is something of a final act after a series of seemingly more mundane prosecutions.

From Dusseldorf to Brooklyn

In February 2013, an individual in Dusseldorf, Germany, called police to report two people loitering in a bank ATM area at night. Police responded and the two individuals—a Dutch carpenter and his 57-year-old mother—were arrested for making a series of fraudulent withdrawals totaling over €160,000. The two were convicted and sentenced to over four years in prison, but remained silent and never divulged how they came to possess the ATM cards and PIN numbers that they used. Their scheme thus seemingly remained a mystery, until it was eventually revealed that they were likely a mini-cashing crew connected to Findikoglu.[4] As it turns out, this mother and son team were the proverbial tip of the iceberg.

On May 9, 2013, the Eastern District announced the unsealing of an indictment charging eight individuals with making multiple fraudulent withdrawals from ATMs throughout New York City.[5] Over a period of hours, the group succeeded in withdrawing a total of $2.8 million. The individuals allegedly comprised yet another cashing crew connected to Findikoglu. In one instance, they purportedly delivered $100,000 to Findikoglu's conspirators in Romania.

The total amount of money withdrawn by this crew—almost all of whom were in their early 20s—ranks as one of the largest heists in New York City history. The charges against them include Access Device Fraud (18 U.S.C. §1029), Money Laundering (18 U.S.C. §1956 and 1957), and forfeiture allegations. A superseding indictment added other defendants and a charge of structuring transactions to evade reporting requirements (32 U.S.C. §5324).

Most of the defendants have pleaded guilty and received relatively modest terms of imprisonment of three years or less, but joint restitution of $2.8 million. The terms of imprisonment imposed on the defendants reflect the fact that the harm caused by each specific individual was relatively limited. The risk for banks, however, is in the aggregate. The New York crew was only one of many such crews operating all over the world, which in total managed to steal $55 million.

Other cashing crews believed to be connected to Findikoglu are gradually being prosecuted. In January 2014, Spanish police arrested six Romanians and two Moroccans who allegedly made 446 withdrawals for €285,000 from two of the banks affected by the Findikoglu hack.[6] In April 2015, Romanian authorities arrested 25 people who allegedly comprised about half of a cashing crew made up of Romanians and other nationalities that succeeded in withdrawing $15 million from ATMs in Japan and Romania.[7] These arrests may well be followed by others connected to Findikoglu.

Mitigating the Risks

The alleged Findikoglu hack and related unlimited operations should cause banks and their processors and vendors to take notice. Banks need to be particularly cautious with vendors and corporations that handle their back-office processing. In the alleged Findikoglu hack, a payment processor in India was purportedly targeted because these processors are perceived as having less secure computer networks than financial services firms. But a hack into a back-office processing vendor can serve as a back door to steal from the clients of the largest and most well-protected financial firms in the world.

Federal Guidance

The Federal Financial Institutions Examination Council (FFIEC) is an organization comprised of the principals of The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee. The alleged Findikoglu unlimited operation prompted it to issue guidance on steps banks can take to mitigate the risks posed by unlimited operations.[8]

The FFIEC cautions that unlimited operations pose "operational risks, fraud losses, liquidity and capital risks, depending on the size of the institution and the losses incurred, and reputation risks." It recommends that banks follow industry standards for data and hardware security. Among other things, it also recommends that banks perform security risk assessments and perform security monitoring, prevention, and risk mitigation.

Although the FFIEC's guidance is directed at banks, any corporation engaged in providing credit or banking services should seriously consider following it. Indeed, as the alleged Findikoglu-related prosecutions were ongoing, the Eastern District successfully prosecuted an international hacker named Qendrim Dobruna.[9] Dobruna was involved in a 2011 unlimited operation and may have been involved with, or at least crossed paths with, individuals involved in the alleged Findikoglu unlimited operations. Like Findikoglu, Dobruna was successfully extradited to the U.S. from Germany. On June 29, 2015, Dobruna was sentenced to 50 months' imprisonment and $14 million in restitution.

Significantly, the charges against Dobruna describe involvement in hacking activity as long ago as 2002. The charges also include allegations that he handled information from hacked E-Bay and PayPal accounts.

In theory, there is no reason why the same technology that is used to carry out ATM unlimited operations could not be used to exploit a variety of financial services. There is no reason why "purchasing crews" could not rack up purchases using hacked credit cards or even pay service account numbers. Currently, retail banks are at the greatest risk of ATM unlimited operations, but in the future other types of corporations will likely become victims of new or hybrid forms of unlimited operations. Corporations that ignore the risk and federal guidance jeopardize their customers, their shareholders and their balance sheets.

Endnotes:

1. Nicholas M. De Feis and Philip C. Patterson, "'Botnets' and the Battle Against Cybercrime," NYLJ, April 30, 2015, available at http://dorlaw.com/pdfs/070051504-2015-Botnet-Article.pdf.

2. See Department of Justice Press Release, "Alleged Mastermind of Global Cybercrime Campaigns Extradited to the United States to Face Charges," June 24, 2015, available at http://www.justice.gov/usao-edny/pr/alleged-mastermind-global-cybercrime-campaigns-extradited-united-states-face-charges.

3. *U.S.A. v. Findikoglu*, 13 CR 440 (E.D.N.Y.).

4. Jörg Diehl, "Alleged mastermind taken from 40-million robbery," Der Spiegel, Aug. 17, 2014, available at http://www.spiegel.de/netzwelt/web/kriminalitaet-im-internet-mutmasslicher-chef-von-cyber-bande-gefasst-a-986388.html.

5. *U.S.A. v. Lajud-Pena*, 13 CR 259 (E.D.N.Y.).

6. Jeremy Kirk, "Spanish police arrest 8 in Bank of Muscat, RAKBANK theft," cnmeonline.com, Jan. 2, 2014, available at www.cnmeonline.com/news/spanish-police-arrest-8-in-bank-of-muscat-rakbank-theft.

7. Lucian Constantin, "Police break up cybergang that stole over $15 million from banks," PCWorld, April 27, 2015, available at http://www.pcworld.com/article/2915112/police-breaks-up-cybergang-that-stole-over-15-million-from-banks.html.

8. FFIEC Joint Statement, "Cyber-attacks on Financial Institutions' ATM and Card Authorization Systems," April 2, 2014, available at https://www.fdic.gov/news/news/financial/2014/fil14010.html.

9. *U.S.A. v. Dobruna,* 12 CR 300 (E.D.N.Y.).