



UNITED STATES ATTORNEY'S OFFICE *Southern District of New York*

U.S. ATTORNEY PREET BHARARA

FOR IMMEDIATE RELEASE
Thursday, April 14, 2016
<http://www.justice.gov/usao/nys>

CONTACT: U.S. ATTORNEY'S OFFICE
Jim Margolin, Dawn Dearden,
Christian Saint-Vil, Nicholas Biase

FBI
Martin Feely, Adrienne Senatore,
Stephanie Shark, Kelly Langmesser
Amy Thoreson

MANHATTAN U.S. ATTORNEY ANNOUNCES CIVIL FORFEITURE COMPLAINT TO RECOVER PROCEEDS OF \$100 MILLION WIRE FRAUD SCHEME

*Complaint Seeks Forfeiture of Funds in At Least 20 Accounts Worldwide Stolen from
American Company Through International Business E-Mail Fraud Scheme*

Preet Bharara, the United States Attorney for the Southern District of New York, and Diego Rodriguez, the Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced today the filing of a civil forfeiture complaint against the funds in at least 20 bank accounts around the world that are alleged to constitute the proceeds of an elaborate scheme to defraud a United States company (the "Victim Company"). In particular, the complaint filed today in Manhattan federal court alleges that the perpetrators of this fraud created a fake email address and posed as one of the Victim Company's legitimate vendors (the "Vendor") in communications with a professional services company (the "Professional Services Company") that the Victim Company retained to handle the details and logistics of vendor payments. Through these fraudulent communications, the perpetrators of the scheme caused the Victim Company to transfer nearly \$100 million due to the Vendor to an account at Eurobank Cyprus, Ltd ("Eurobank") that was actually under their control. Almost immediately after funds were transferred into this account, the perpetrators of this scheme caused portions of the fraud proceeds to be further dispersed to accounts under their control around the world, including in Latvia, Estonia, Hungary, Lithuania, Slovakia, Estonia, and Hong Kong.

Through the timely actions of officials at Eurobank, and in coordination with U.S. and Cypriot law enforcement authorities, more than \$74 million of the stolen funds have already been returned to the Victim Company. Foreign governments acting at the request of U.S. authorities have restrained 20 accounts worldwide that received portions of the remaining ill-gotten funds, and the funds in those accounts are the subject of the complaint filed today in Manhattan federal court.

Manhattan U.S. Attorney Preet Bharara said: “Criminals can be resourceful and unrelenting in their efforts to scam innocent victims out of money. Here, the alleged perpetrators – through a fake email address and by impersonating a legitimate vendor – almost got away with \$100 million. Thanks to the timely actions of law enforcement here and abroad, as well as by Eurobank in Cyprus, where the stolen funds were first sent, \$74 million has already been returned to the victim company. With this civil forfeiture action, we seek to return the rest.”

FBI Assistant Director-in-Charge Diego Rodriguez, said: “This modern-day impersonation scheme used a fake email account to scam a business instead of the old way of impersonation by the perpetrators. However, this scam was cut short in the end thanks to modern-day tools used by banks to stop suspicious transactions and cooperation by our foreign partners to restrain the transferred funds.”

As alleged in the Complaint:

The Victim Company is an American-based corporation doing business worldwide. Like many corporations, the Victim Company has contractors and vendors who are paid via wire transfer for services provided, including the Vendor, which is based in Asia. During all times relevant to the Complaint, the Victim Company retained the Professional Services Company to communicate with vendors and handle the details of vendor payments.

Over the course of several weeks in August and September 2015, the perpetrators of the scheme described in the Complaint managed to impersonate the Vendor by creating a fake email address that resembled email addresses used by actual employees of the Vendor. Using this fake email address, the perpetrators then communicated with an email account maintained for the purpose of allowing vendors to communicate with the Professional Services Company on behalf of the Victim Company. Through those email communications, the perpetrators of the scheme convinced the Professional Services Company to change the designated bank account to which the Victim Company would make recurring payments to the Vendor for services rendered. As a result, payments from the Victim Company meant for the Vendor were transferred to an account under the control of the perpetrators of this scheme (“Subject Account-1”) rather than an account actually affiliated with the Vendor.

Once this change was put into effect, the Professional Services Company, on behalf of the Victim Company, began directing a series of payments from Victim Company accounts in the United States to Subject Account-1 that were intended for the Vendor. Specifically, between August 21, 2015, and September 14, 2015, approximately 16 payments intended for the Vendor as payment for services rendered to the Victim Company were wired for deposit into Subject Account-1, totaling approximately \$98,879,545.80. Officials at Eurobank developed concerns regarding these transfers and, as a result, restrained approximately \$74 million of the transferred funds before they settled into Subject Account-1. In coordination with law enforcement authorities, those funds have since been returned to the Victim Company.

In regard to the approximately \$25 million that actually settled into Subject Account-1, the perpetrators of the scheme then laundered portions of those crime proceeds through at least

19 additional accounts, including accounts in Cyprus, Latvia, Hungary, Estonia, Lithuania, Slovakia, and Hong Kong. Those accounts, along with Subject Account-1, have since been restrained by foreign governments acting at the request of U.S. authorities.

* * *

Mr. Bharara praised the outstanding investigative work of FBI. He also thanked the Financial Crimes Enforcement Network (“FinCEN”) of the United States Department of the Treasury, the Law Office of the Republic of Cyprus Unit for Combating Money Laundering, and Eurobank Cyprus Ltd. for all of their assistance in the investigation and the return of funds to the Victim Company.

This investigation is being handled by the Office’s Money Laundering and Asset Forfeiture Unit and Complex Frauds and Cybercrime Unit. Assistant United States Attorneys Edward B. Diskant and Megan L. Gaffney are in charge of the case.

The investigation is ongoing.

16-087

###