SEALED

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
MAY 26 2016
CLERK, U.S. DISTRICT COURT
By _____ Deputy

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA

v.

MARTAVIOUS BANKS KEYS

NO. 3:16-MJ-459-BH

FILED UNDER SEAL

GOVERNMENT'S APPLICATION FOR ORDER DIRECTING THE DEFENDANT TO UNLOCK A CELLULAR TELEPHONE USING HIS FINGERPRINTS

TO THE HONORABLE JUDGE OF SAID COURT:

COMES NOW the United States of America, by and through the United States Attorney for the Northern District of Texas, and files this it's Government's Application for Order Directing the Defendant to Unlock a Cellular Telephone Using His Fingerprints, pursuant to Title 28 U.S.C. §1651, and would show the following:

I.

Martavious Keys (Suspect) is a suspect in an investigation involving sex trafficking of minors, in violation of Title 18 U.S.C. §§ 1591(a) and a felon in possession of a firearm investigation, in violation of Title 18 U.S.C. § 922(g)(1). During the course of the investigation, a federal arrest warrant was issued for Martavious Keys pursuant to a criminal complaint. The warrant was executed on May 19, 2016. At the time of his arrest, Keys was in possession of an Apple iPhone Model 5S, IMEI 579C-E2642B, with an FCC ID BCG-E2642A, which is white and gold in color, equipped with the "Touch ID." The Government presented a search warrant affidavit for the aforementioned Apple iPhone, which was granted by this Court.

Beginning with the release of iOS 8 (the operating system for Apple mobile devices) in September 2014, Apple no longer has a key to decrypt these devices. Thus, even with a properly authorized search warrant to gain access to the content of an iOS device, there is no feasible way for the government to search the device.

According to publicly available materials published by Apple, the iPhone 5S is equipped with "Touch ID," a feature that recognizes up to five fingerprints designated by the authorized user of the iPhone. A Touch ID sensor, a round button on the iPhone or iPad, can recognize fingerprints. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode. Furthermore, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone. Similarly, Touch ID will not allow access if the device has been turned on or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. For these reasons, it is necessary to use the fingerprints and thumbprints of any device's users to attempt to gain access to any Apple devices found while executing the search warrant or immediately afterward. The government may not be able to obtain the contents of the Apple devices if

those fingerprints are not used to access the Apple devices by depressing them against the Touch ID button.

The undersigned attorney for the Government has spoken with several cellular telephone forensics experts, and they all stated that they are unaware of any method to forensically circumvent or bypass the Touch ID or passcode. In short, if the suspect does not provide his fingerprint on the Touch ID sensor or his passcode, it is impossible, at this time, to access the phone and any evidence which may have been found on it will be lost.

II.

The Supreme Court has explicitly endorsed the use of the All Writs Act to ensure that a court's search warrants are not frustrated. The Court held that the All Writs Act permits federal courts to "issue such commands… as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained." *United States v. New York Tel. Co.,* 434 U.S. 159, 172 (1977).

The Government is asking the Court to use its power under the All Writs Act to compel the suspect to unlock his iPhone using his fingerprint. The Fifth Amendment's protection against self-incrimination "applies only when the accused is compelled to make a testimonial *communication* that is incriminating." *Baltimore City Dept. of Social Services v. Bouknight,* 493 U.S. 549, 554 (1990). (emphasis added). A communication is testimonial when it "explicitly or implicitly, relate[s] a factual assertion or disclose[s] information." *Id.* A communication is non-testimonial when a person is "not required to disclose any knowledge he might have, or to speak his guilt." *United States v. Doe,* 487

U.S. 201, 210 (1988). Thus, "certain acts, though incriminating, are not within the privilege" against self-incrimination, because they are not communications at all. *Id.* A person's fingerprint does not require him to make any factual assertions or disclose any information. The taking of fingerprint samples does not violate any right of the suspect (*Schmerber v. State of California*, 86 S.Ct. 1826, 1832 (1966), and does not fall within the category of communications or testimony so as to be protected by the Fifth Amendment. *United States v. Gibson*, 444 F.2d 275, 277 (5th Cir. 1971).

At least one court has addressed this issue and come to the same conclusion. David Charles Baust was charged by indictment with violating Code of Virginia § 18.2-51.6, Strangling Another Causing Wounding or Injury. *Virginia v. Baust*, 2014 WL 6709960 (Va.Cir.Ct. 2014). During the course of the investigation, the police secured a search warrant for Baust's iPhone, which they believed to contain video evidence of the strangulation. The state sought to compel Baust to unlock his phone using his fingerprint and to provide his passcode. The court held that providing a fingerprint was non-testimonial, and Baust could therefore be compelled to place his fingerprint on the Touch ID sensor to unlock the phone. The court reasoned that "[T]he privilege offers no protection against compulsion to submit to fingerprinting, photography, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture. Even though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. The act of exhibiting such physical characteristics is not the same as a sworn communication by a witness that relates

either express or implied assertions of fact or belief." *Id.* The court did find, however, distinguish between providing a fingerprint and providing a passcode. The court found that providing a passcode was a testimonial communication since it required Baust to divulge something that he knew, so the 5th Amendment prohibited the state from compelling him to provide it.

III.

WHEREFORE, premises considered, the Government requests that the Court order the defendant, Martavious Keys, to allow investigators to attempt to unlock his Apple iPhone Model 5S, IMEI 579C-E2642B, with an FCC ID BCG-E2642A, which is white and gold in color, using his fingers/thumbs and fingerprints/thumbprints.

Respectfully submitted,

JOHN R. PARKER
UNITED STATES ATTORNEY

CARA FOOS PIERCE
Assistant United States Attorney
Bar No. 24036579
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8678
Facsimile: 214-767-4100
Email: Cara.Pierce@usdoj.gov