UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

MICHAEL RANDO, et al.,

Defendants.

Case 3:22-cv-487-TJC-MCR

PLAINTIFF'S RESPONSE IN SUPPORT OF RECEIVER'S MOTION FOR ORDER TO SHOW CAUSE (DOC. 40)

Defendants refuse to comply with this Court's Order to provide the Receiver access to two email accounts, claiming the contents of those accounts would incriminate them. The FTC agrees in part with Defendants' position – the contents of those accounts are indeed likely to incriminate them.[1] However, it is well settled the Fifth Amendment does not apply to incriminating documents such as these which were voluntarily prepared. *See United States v. Hubbell*, 530 U.S. 27, 35 (2000). Moreover, Defendants' act of providing access to these accounts does not communicate any incriminating fact that is not a "foregone conclusion" in light of Defendants' declarations describing these accounts and other documents and information already in the hands of the FTC and the Receiver. *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1341 (11th Cir. 2012) (quoted source omitted).

[1] The FTC's TRO Motion (Doc. 4) and Supplemental Filing ISO PI (Doc. 28) catalogue numerous pieces of evidence demonstrating Defendants defrauded consumers and misled CRAs and potential creditors in violation of Section 5 of the FTC Act, CROA, TSR, and BOR.

Accordingly, the Fifth Amendment does not relieve Defendants from the Order to provide access to these accounts, and their refusal to do is contempt of Court.

I. BACKGROUND

The Court ordered Defendants to "provide the Receiver with shared access to the accounts at issue until the business and personal affairs can be separated." (Doc. 35.) The Court also ordered Defendants to "produce all historic documents and communications in the accounts pertaining to the Receivership Entities and to provide a complete forensic image of the accounts." (*Id.*) To date, Defendants have refused to comply, instead claiming a Fifth Amendment privilege in opposition (Doc 49) to the Receiver motion to comply with the Court's order (Doc. 40).

II. ARGUMENT

Defendants argue requiring them to give access to their email accounts would violate their Fifth Amendment privilege because the content of the documents the Court ordered them to share would be incriminating. This argument, however, misconstrues the Fifth Amendment. The right against self-incrimination "applies only when the accused is compelled to make a Testimonial Communication that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976) (emphasis added); *see In re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1341. In other words, the privilege applies where responding to a discovery request would require Defendants to *create* documents that would incriminate them. "[T]he Supreme Court has consistently held the Fifth Amendment does not apply to the contents of voluntarily prepared and previously generated documents, even though they may contain

incriminating information." *FTC v. PointBreak Media, LLC*, 343 F. Supp. 3d 1282, 1286 (S.D. Fla. 2018) (citing *Hubbell*, 530 U.S. at 35).

Here, the Court's Order does not compel Defendants to create incriminating documents, merely provide access to the email accounts, which contain preexisting documents. The incriminating nature of these preexisting documents is not sufficient to justify Defendants' assertion of the Fifth Amendment privilege. *See id.* at 1292 (rejecting defendants' claim of Fifth Amendment privilege and requiring turnover of their cellphones and laptops to the Receiver for imaging).

The Fifth Amendment privilege can only protect Defendants if the act of providing those documents, not their contents, is itself incriminatory. *Fisher*, 425 U.S. at 410 ("The act of producing evidence . . . has communicative aspects of its own, wholly aside from the contents of the papers produced."). Under this longstanding principle, courts have upheld the privilege where the act of providing the documents necessarily incriminated a defendant by effectively conceding the existence, authenticity, and control of those documents. *See Hubbell*, 530 U.S. at 36. The act of production, however, cannot provide the basis for a successful assertion of the Fifth Amendment when elements like existence, authenticity and control "are a foregone conclusion." *Id.* at 44-45; *Fisher,* 425 U.S. at 410-11.

When those elements are a forgone conclusion, the question is "not of testimony but of surrender," and the Fifth Amendment does not apply. *Fisher,* 425 U.S. at 411. While the FTC may not rely on mere conjecture, it need only establish existence, authenticity, and control with "reasonable particularity." *In re Grand Jury*

Subpoena Duces Tecum, 670 F.3d at 1349 n.28. With respect to existence, "the Government need not know the name of a particular file or account" and must only show "that a file or account, whatever its label, does in fact exist." *Id. See also Apollo Endosurgery, Inc. v. Ka fka,* No. 15-CV-23757, 2016 WL 7470003, at *3 & n.7 (S.D. Fla. Mar. 15, 2016) (finding that knowledge that defendant has inventory of product and is selling them meets "reasonable particularity" requirement for document request calling for "[a]ll documents regarding the sale" of the product).

Here, both the FTC and the Receiver already know the email accounts it seeks exist, the accounts belong to Defendants, and Defendants can access them. Indeed, Defendants expressly concede the elements in declarations filed with the Court. Specifically, Mr. Rando concedes he "created the Mikesingles@gmail.com email account" and uses the accounts to this day to communicate regarding daily matters such as communicating with "medical professionals about ongoing care, with daycares, schools, nannies, friends, family, to pay bills and monitor" personal financial and social media accounts. (Doc. 31-1 ¶¶ 2, 4.) Ms. Rando admits to the same with respect to her "Val.10xlife@gmail.com email account." (Doc. 31-2 ¶¶ 2, 4.) With respect to the accounts' contents, both Mr. and Mrs. Rando admit they have used the accounts not only for their personal purposes but also "for business purposes, including to monitor various business accounts relating to the Receivership Entities." (Doc. 31-1 ¶ 3; Doc. 31-2¶ 3.) Moreover, Defendants' organization chart, obtained during the immediate access on their business premises, identifies the Mikesingles@gmail.com and Val.10xlife@gmail.com accounts as the primary

business emails for Mr. and Mrs. Rando, respectively. (PX140.) Additionally, the Receiver's efforts have uncovered business accounts that use the two email accounts at issue. (Doc. 29-1 ¶ 8.) Indeed, a search of the accessible business documents obtained throughout the FTC's investigation and this litigation returned 2,047 documents referencing the Mikesingles@gmail.com email account and 704 documents referencing the Val.10xlife@gmail.com email account. (PX147 (redacted screenshots of search results on FTC's Relativity database).)

Thus, Defendants' compliance with the Court's order does not reveal any information that they have not already admitted in this proceeding, "adds little to nothing to the sum total of the Government's information," and thus would not implicate the Fifth Amendment. *Fisher*, 425 U.S. at 411. *See also United States v. Bright*, 596 F.3d 683, 693 (9th Cir. 2010) (foregone conclusion exception applies to production of documents related to two credit card accounts expressly named in the IRS summonses but not to two other credit card accounts the IRS could not expressly name) (citing *In re Grand Jury Subpoena*, 383 F.3d at 910).

None of the cases cited by Defendants supports a different result. In *In re Grand Jury Subpoena Tecum*, the Eleventh Circuit declined to apply the foregone conclusion doctrine to computer hard drives, but only because evidence did not establish "that encrypted files exist on the drives, that [the defendant] has access to those files, or that he is capable of decrypting the files." 670 F.3d at 1339. Thus, that precedent does not apply when "the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that [the defendant]

can access them." *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (applying *In re Grand Jury Subpoena Tecum*). As detailed above, it is undisputed the two email accounts contain emails and Defendants can access the accounts.

Defendants also discuss *In re Boucher*, No. 2:06-MJ-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009), but mischaracterize it to suggest the Court can only apply the foregone conclusion doctrine to compel the production of specific documents of which the Receiver has direct knowledge. (Doc. 49 at 7 (stating that the *Boucher* court only required "the production of the unencrypted files that the government agents had already viewed").) Not so. The *Boucher* court directed the production of the *entire* drive in its unencrypted form, even though government agents had only "viewed the contents of *some* of the Z drive's files" and had "not viewed most of the files on the Z drive." *In re Boucher*, 2009 WL 424718, at *3. In other words, the court required the defendant to produce the majority of the drive's files, which the government never viewed, based on *circumstantial* evidence of their existence and nature.

Under *Boucher,* the foregone conclusion doctrine applies here because of the circumstantial – and direct – evidence the FTC and the Receiver have collected regarding the existence and nature of the documents contained in the accounts, evidence confirmed by Defendants' own admissions.

Finally, Defendants cite *SEC v. Complete Bus. Sols. Grp., Inc.* for the proposition that the Receiver must "demonstrate with 'reasonable particularity' that [s]he is

aware of the materials [s]he is seeking" in order for the foregone conclusion doctrine to apply. No. 20-CIV-81205-RAR, 2022 WL 1288749, at *2 (S.D. Fla. Apr. 29, 2022), *motion to certify appeal denied*, No. 20-CV-81205-RAR, 2022 WL 1522078 (S.D. Fla. May 13, 2022). Tellingly, Defendants fail to mention the receiver in that case only provided information from the defendants' financial disclosure statement which identified the defendants' assets. The court found this limited information established a foregone conclusion with "reasonable particularity" to justify the receiver's broad request for "*any* documents in [defendant's] possession, custody, or control" that pertain not just to the identified assets, but to any asset that falls within any of "10 *categories* of assets" listed in the financial disclosure form. *Id.* (emphasis added). Again, the FTC and the Receiver have considerably more evidence here identifying the universe of relevant accounts (the two email accounts) and the nature of the documents they contain.

Defendants do not dispute they violated the Turnover Order. They also do not dispute the "violated order was valid and lawful; . . . the order was clear and unambiguous; and [they] . . . had the ability to comply." *FTC v. Leshin*, 618 F.3d 1221, 1232 (11th Cir. 2010) (ellipses in original) (internal citation and quotation omitted). Moreover, under the clear record developed here, the Fifth Amendment does not excuse Defendants' refusal to comply with this Court's Order. Any testimonial value in Defendants' providing access to the two email accounts is a foregone conclusion in light of their declarations describing the same and other evidence obtained by the FTC and the Receiver. Accordingly, Defendants are in

clear contempt of this Court and are appropriately subject to sanctions. *See SEC v. Yun,* 208 F.Supp.2d 1279, 1288 (M.D. Fla. 2002) ("Without the power to punish noncompliance with its orders, this Court's authority to issue judgments would be nothing more than a mere mockery."). Therefore, a coercive sanction, sufficient to compel Defendants' compliance, is warranted.[2] *See Int'l Union, United Mine Workers of Am. v. Bagwell*, 512 U.S. 821, 828 (1994) (finding incarceration as "the paradigmatic coercive, civil contempt sanction" and recognizing the contemnor "carries the keys of his prison in his own pocket" because he can end incarceration at any time through his compliance).

Dated: June 15, 2022

Respectfully submitted,

/s/ Hong Park

Hong Park, hpark@ftc.gov (202-326-2158)
Brian M. Welke, bwelke@ftc.gov (-2897)
Sana Chaudhry, schaudhry@ftc.gov (-2679)
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue NW, CC-9528
Washington, DC 20580
Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

[2] While the FTC submits to the Court's discretion regarding whether incarceration as opposed to a daily fine would be the most effective sanction to ensure Defendants' compliance, imposition of a daily fine risks dissipating any funds available for consumer redress in this matter, should the FTC prevail.

CERTIFICATE OF SERVICE

I hereby certify that on June 15, 2022, I served a true and correct copy of the foregoing via CM/ECF to those listed on the CM/ECF system.

/s/ Hong Park
Hong Park