

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 18-CIV-80176-Bloom/Reinhart

IRA KLEIMAN, as personal representative of
the estate of David Kleiman, and
W&K INFO DEFENSE RESEARCH, LLC,

Plaintiffs,

v.

CRAIG WRIGHT,

Defendant.

ORDER ON PLAINTIFFS' MOTION TO COMPEL [DE 210]¹

This matter is before the Court on the Plaintiffs' Motion to Compel, DE 210, and the Court's Order dated June 14, 2019. DE 217. The Court has considered the totality of the docketed filings, including all pleadings referenced herein and transcripts of all cited court proceedings. As the judicial officer who presided at the relevant proceedings, I retain a current and independent recollection of the events discussed below. I have reviewed all of the exhibits introduced into the record at the evidentiary hearing, including the deposition excerpts filed in the record. *See* DE 270. Finally, I have carefully considered the arguments of counsel. The Court is fully advised and this matter is ripe for decision. The Court announced its ruling from the bench on August 26,

¹ Magistrate judges may issue an order on any "pretrial matter not dispositive of a party's claim or defense." Fed. R. Civ. P. 72(a). "Thus, magistrate judges have jurisdiction to enter sanctions orders for discovery failures which do not strike claims, completely preclude defenses or generate litigation-ending consequences." *Wandner v. Am. Airlines*, 79 F. Supp. 3d 1285, 1295 (S.D. Fla. 2015) (J. Goodman).

2019. This Order memorializes that ruling. To the extent the relief granted in the written Order deviates from the oral pronouncement, the Order controls.

Two preliminary points. First, the Court is not required to decide, and does not decide, whether Defendant Dr. Craig Wright is Satoshi Nakamoto, the inventor of the Bitcoin cybercurrency.² The Court also is not required to decide, and does not decide, how much bitcoin, if any, Dr. Wright controls today. For purposes of this proceeding, the Court accepts Dr. Wright's representation that he controlled (directly or indirectly) some bitcoin on December 31, 2013, and that he continues to control some today.

PROCEDURAL HISTORY

This case arises from a dispute over the ownership of bitcoin and Bitcoin-related intellectual property. Plaintiffs allege in the Second Amended Complaint that David Kleiman and Dr. Wright were partners in the creation of the Bitcoin cybercurrency and that they "mined" (i.e., acquired) a substantial amount of that currency together. DE 83. Dr. Wright denies any partnership with David Kleiman, and further denies that David Kleiman had an ownership interest in the bitcoin that was mined. Alternatively, Dr. Wright asserts that David Kleiman transferred any interest he had in the bitcoin and the intellectual property to Dr. Wright in exchange for equity in a company that ultimately failed. *See* DE 87. David Kleiman died in 2013.

As early as July 2018, Plaintiffs sought discovery to identify the bitcoin that Dr. Wright owned and controlled (his "bitcoin holdings"). In Ira Kleiman's First Set of Interrogatories served on July 31, 2018, he asked Dr. Wright to identify "public keys and public addresses" for any cryptocurrency he currently or previously owned. DE 91-2 at 8. Dr. Wright responded on

² A note on terminology. Unless otherwise specified, when I refer to units of the cybercurrency, I will use the lower-case "bitcoin" (like "dollars"). When I refer to the particular cybercurrency system, I will use the upper-case "Bitcoin" (like "the U.S. Dollar").

February 1, 2019, by objecting that the discovery request was “irrelevant, grossly overbroad, unduly burdensome, harassing and oppressive, and not proportional to the needs of the case.” DE 91-2 at 14-19.³ Under the procedures required by my Standing Discovery Order (DE 22, 102), the parties requested a discovery hearing to resolve their respective objections. That hearing was scheduled for February 20, 2019. DE 90.

Dr. Wright submitted his pre-hearing memorandum on February 14, 2019. DE 92. He noted that Plaintiffs had requested all documents relating to any bitcoin transactions by Dr. Wright between 2009 and 2014. *Id.* at 3. Dr. Wright argued that the discovery requests were disproportionate to the needs of the case. He represented that he “stands ready to produce documents in his possession, custody, or control that relate to Dave [Kleiman], any trust in which Dave [Kleiman] was a trustee or beneficiary, and W&K Info Defense Research, LLC.” *Id.* at 4.

At the hearing on February 20, the Court and the parties had a discussion about Plaintiffs’ request for evidence relating to Dr. Wright’s bitcoin transactions. DE 123 at 120-123 (hearing transcript). I declined to order Dr. Wright to produce his current bitcoin holdings. Rather, I said Plaintiffs should identify a starting date and seek production of Dr. Wright’s bitcoin holdings on that date. Plaintiffs could use the Bitcoin evidence trail to trace forward from there.

Running in parallel with the interrogatories, Plaintiffs served a Second Set of Requests for Production on Dr. Wright on or about January 17, 2019. DE 92-5 at 30. Request for Production #1 sought “All documents or communications that provide and/or estimate the value of your cryptocurrency holdings. This includes, but is not limited to, loan applications, financial statements, tax returns, life insurance applications, financing agreements, sale papers, assignment contracts, etc.” 2 DE 114-1 at 5-6. On February 19, Dr. Wright served a written objection to

³ Discovery was stayed from August 2, 2018, to December 31, 2018. DE 57, 72.

Request #1 based on relevance, over-breadth, harassment, and disproportionality. *Id.* at 5-6. The parties conferred but were unable to resolve the objection. *Id.* at 7. A discovery hearing was scheduled for March 6, 2019. DE 104.

On March 4, the parties submitted their Joint Discovery Memorandum. DE 109. They indicated that Plaintiffs' Request for Production #1 was still in dispute. *Id.* at 7. The hearing was held on March 6. DE 110, DE 122 (hearing transcript). The parties deferred the Request for Production issue to the next discovery hearing. DE 122 at 56. Plaintiffs explained that they were revising the Request for Production related to Dr. Wright's bitcoin holdings: "We have chosen – we have moved everything back to 2013, which is when Dave died. You Honor will have an opportunity to hear from both sides, but we basically said give us the information as of that date and then we will move forward from there." *Id.* at 62. Another discovery hearing was set for March 14.

On March 13, the parties submitted their Joint Discovery Memorandum for the March 14 discovery hearing. DE 114. Plaintiffs represented that they had "limited the request to: 'produce any documents that existed as of 12/31/13 which estimate the value of Defendant's bitcoin holdings.'" *Id.* at 3. Plaintiffs argued that this information was relevant to trace the assets of the alleged partnership between David Kleiman and Dr. Wright. *Id.* Dr. Wright argued that, even as limited, the request was "overly broad, unduly burdensome and harassing by seeking such personal financial information such as loan applications, financial statements, tax returns, life insurance applications, etc." *Id.*

At the hearing on March 14, Plaintiffs further explained that the purpose of this request for production was to help establish the universe of bitcoin that was mined during the alleged Kleiman-Wright partnership. DE 124 at 18-19 (hearing transcript). Plaintiffs agreed that what they were

really seeking was “a listing of all the bitcoin that was owned [by Dr. Wright directly or indirectly] on December 31, 2013.” *Id.* at 19-20. Dr. Wright objected on relevance grounds. The Court found “what bitcoin existed on December 31, 2013, and where it’s gone since then is relevant to [Plaintiffs’] claim.” *Id.* at 21. Turning to proportionality and undue burden, the Court asked Dr. Wright’s counsel, “[H]ow difficult would it be to come up with information? I assume it’s just a list of Bitcoin wallets from December 2013.” *Id.* at 21. Dr. Wright’s counsel responded, “Well, it’s a list of – it would be a list of public addresses, but it would identify Craig Wright as being the owner of those addresses, which sort of like opens the door to, you know, a lot of financial information, and without any evidence that all of those — or what portion of those Dave Kleiman had an interest in.” *Id.*

The Court ruled that Plaintiffs were entitled to a list of Dr. Wright’s bitcoin holdings, but granted Dr. Wright leave to file a motion for protective order based on undue burden. *Id.* at 22-23. Notably, the Court did not specify the information Dr. Wright was required to use to generate the list. Specifically, the Court did not order production of a list of public addresses. The Court did not set a specific deadline for production or for the filing of the motion for protective order.

Dr. Wright was deposed on April 4. During his deposition, he testified that a trust called the Tulip Trust was formalized in 2011, but never owned or possessed private keys to bitcoin addresses. DE 270-1 at 22. He also testified that Uyen Nguyen had ceased to be a trustee of any trust related to Dr. Wright in 2015. *Id.* at 24. He further testified that he had stopped mining bitcoin in 2010. He declined to answer questions about how much bitcoin he mined in 2009-2010; this issue was reported to the Court during the deposition. I deferred ruling on the issue. DE 137 at ¶ 1 (“The request to compel Dr. Wright to disclose the amount of bitcoin he mined during 2009 and 2010 is denied without prejudice. The Court will revisit this issue after the parties brief

whether production of a list of Dr. Wright's bitcoin ownership would be unduly burdensome.”). Again, the Court referenced “a list of Dr. Wright's bitcoin ownership.” The Court did not mention a list of public addresses.

A discovery hearing was held on April 11. DE 142. At that hearing, I set a deadline of April 19 for Dr. Wright to file a motion regarding Plaintiffs' request for a list of his bitcoin holdings on December 31, 2013. DE 146 at 38-39 (hearing transcript).

On April 18, Dr. Wright filed a Sealed Motion Regarding Production of a List of the Public Addresses of his Bitcoin as of December 31, 2013. DE 155.⁴ Dr. Wright incorrectly framed the issue as, “The Court has ordered Dr. Wright to identify all public addresses that he owned as of December 31, 2013 or, if he cannot do so, explain why identification is unduly burdensome.” *Id.* at 1. He then stated:

Dr. Wright does not have a complete list of the public addresses that he owned as of any date. To create such a list would be unduly burdensome. A Bitcoin public address is an identifier of 26-35 alphanumeric characters. Such addresses are not intended to be memorized and remembered for a period of nearly a decade. However, Dr. Wright knows that he mined the [REDACTED] on the blockchain. Because the public addresses associated with blocks are publicly available, Dr. Wright is able to identify the public addresses associated with the [REDACTED] blocks on the blockchain and provides those public addresses below. [REDACTED] Dr. Wright did not keep track of which Bitcoin blocks he mined. Dr. Wright does not know any of the other Bitcoin public addresses.

In 2011, Dr. Wright transferred ownership of all of his Bitcoin into a blind trust. Dr. Wright is not a trustee or a beneficiary of the blind trust. Nor does Dr. Wright know any of the public addresses which hold any of the bitcoin in the blind trust. Thus, Dr. Wright does not know and cannot provide any other public addresses.

First, as of December 31, 2013, all of Dr. Wright's bitcoin had been transferred to the blind trust, and therefore are owned by the trusts, not by Dr. Wright. The public addresses referenced above are as follows:

⁴ The motion was filed under seal. A redacted version of the motion is filed in the public record at Docket Entry 184.

[REDACTED]⁵

DE 184 at 1-2. As shown above, the Court had not ordered Dr. Wright to produce a list of public addresses. Dr. Wright did not assert, then, that public addresses were a meaningless data point. He simply argued that he could not produce them.

Plaintiffs filed a response in opposition to the Motion. DE 162.⁶ They sought an order requiring Dr. Wright to identify all bitcoins he owned as of December 31, 2013, to provide the trust documents, and to provide a sworn statement identifying all bitcoins he transferred to the blind trust as well as the identities of the trustees and trust beneficiaries. DE 183 at 5-6.

The Court denied Dr. Wright's Motion on May 3, 2019. DE 166. After reviewing the procedural history, the Court stated:

Thereafter, Dr. Wright filed an unverified motion in which he identified a number of bitcoin public addresses that he mined. Although not delineated as a Motion for Protective Order, that is what the pleading is. Dr. Wright asserted that he does not have a complete list of the public addresses he owned on any date, including December 31, 2013. He further asserted that in 2011 he transferred ownership of all his bitcoin to a blind trust. Although he makes the conclusory statement that it would be unduly burdensome to produce a list of his bitcoin holdings as of December 31, 2013, this conclusion is not supported by facts. In essence, he does not argue undue burden, he argues impossibility. The argument that Dr. Wright is incapable of providing an accurate listing of his current or historical bitcoin holdings was never presented in any of the prior hearings before this Court, when the Court was crafting the scope of discovery. Notably, [Dr. Wright's motion] does not refute the obvious response to this argument – get the information from the trustee of the blind trust.

DE 166 at 2-3. Again, the Court referenced a “listing of” Dr. Wright's bitcoin holdings, not a list of public addresses. The Court ordered:

⁵ Dr. Wright produced a partial list of bitcoin public addresses that he mined prior to 2011. DE 155 at 2-3.

⁶ The Response was filed under seal. A redacted version is filed in the public record at Docket Entry 183.

- On or before May 8, 2019, at 5:00 p.m. Eastern time, Dr. Wright shall provide to Plaintiffs a sworn declaration identifying the name and location of the blind trust, the name and contact information for the current trustee and any past trustees, and the names and contact information of any current or past beneficiaries.
- On or before May 9, 2019, at 5:00 p.m. Eastern time, Dr. Wright shall produce to Plaintiffs a copy of any and all documents relating to the formation, administration, and operation of the blind trust. The production shall be accompanied by a sworn declaration of authenticity.
- On or before May 15, 2019, at 5:00 p.m. Eastern time, Dr. Wright shall produce all transactional records of the blind trust, including but not limited to any records reflecting the transfer of bitcoin into the blind trust in or about 2011. The production shall be accompanied by a sworn declaration of authenticity.
- Dr. Wright shall execute any and all documents, or other legal process, necessary to effectuate the release of documents in the possession, custody, or control of the Trustee.

Id. at 4.

Defendant's counsel sought an extension of time to comply with the May 3 Order so that they could fly to London to meet with their client in person to prepare the required declaration. DE 167. That request was granted. DE 195 (Telephonic Hearing Transcript), DE 172.

Dr. Wright provided a sworn declaration dated May 8, 2019. DE 222.⁷ He swore that he had met with his counsel in person on May 7 and 8 to "provide them with additional details and clarity regarding trusts that I settled that hold or held Bitcoin that I mined or acquired on or before December 31, 2013." DE 222 at ¶ 3. Dr. Wright further swore:

- In 2009 and 2010 he had mined bitcoin directly into a trust in Panama, that there were no transactions related to those bitcoin, and that he later "transferred the encrypted files that control access to these Bitcoin in 2011, as explained below." *Id.* ¶ 4.
- In June 2011, he consolidated "the Bitcoin that I mined with Bitcoin that I acquired and other assets." *Id.* ¶ 5.

⁷ A sealed copy was filed at DE 223. A redacted copy was filed at DE 222.

- To that end, “[i]n October 2012, a formal trust document was executed, creating a trust whose corpus included the Bitcoin that I mined, acquired and would acquire in the future. The name of that trust is Tulip Trust. It was formed in the Seycelles [sic].” *Id.*
- The trustees of Tulip Trust I are COIN Ltd. UK., Uyen Nguyen, Dr. Wright, David Kleiman, Panoptcrypt Pty. Ltd, and Savannah Ltd. *Id.* ¶ 6. Dr. Wright is the contact person for COIN Ltd. UK. The contact person for Panoptcrypt Pty. Ltd. is Dr. Wright’s wife. The contact person for Savannah Ltd. is Denis Mayaka. *Id.* ¶¶ 9-12.
- The beneficiaries of Tulip Trust I are Wright International Investments Ltd. and Tulip Trading Ltd. Dr. Wright is the point of contact for both of the beneficiaries. *Id.* ¶¶ 13-14.
- A second Tulip Trust exists. Dr. Wright and his wife are the beneficiaries. *Id.* at ¶¶ 19-20.
- “Access to the encrypted file that contains the public addresses and their associated private keys to the Bitcoin that I mined, requires myself and a combination of trustees referenced in Tulip Trust I to unlock based on a Shamir scheme.” *Id.* at ¶ 23.

He also provided certain documents related to the trust.⁸

On June 3, Plaintiffs filed a Motion to Compel Defendant to Comply with this Court’s Orders Directing Him to Produce a List of the Bitcoins He Held as of December 31, 2013. DE 197 (sealed) (redacted version filed at DE 210). Plaintiffs asked the Court to impose sanctions under Rule 37 and to order Dr. Wright to provide a sworn statement identifying the public addresses of the bitcoin transferred into the Tulip Trusts, to provide transactional records and communications relating to the trusts, and to sit for a renewed deposition. DE 210 at 6. Although

⁸ Plaintiffs represent, “In response to the Court’s order, Craig produced two sworn statements, copies of various trust instruments, and a statement from the purported trustee re-attaching a trust instrument.” DE 210 at 3. Dr. Wright’s Response states that he “produced trust formation documents along with a sworn declaration of authenticity,” as well as “documents reflecting the use of bitcoin rights from the trust to support research and development by his Australian entities.” DE 211 at 3.

the Plaintiffs “defer[red] to the Court’s judgment as to the appropriate sanction,” they requested that if Dr. Wright continued to refuse to comply that the Court deem all of Dr. Wright’s holdings in the Tulip Trust to be joint property belonging to both Dr. Wright and David Kleiman. DE 210 at 6; DE 221 at 15.

In his response, Dr. Wright conceded that he has not complied with the Court’s order, but argued that compliance was impossible. DE 204 (redacted version filed at DE 211). Expanding on the representation made in Paragraph 23 of his declaration, he argued that information necessary to produce a complete list of his bitcoin holding on December 31, 2011, was in the Tulip Trust I in a file that is encrypted using “‘Shamir’s Secret Sharing Algorithm’, an algorithm created by Adi Shamir to divide a secret, such as a private encryption key, into multiple parts.” DE 211 at 5. Dr. Wright asserted that he could not decrypt the outer level of encryption because he did not have all of the necessary decryption keys. *Id.* He stated that after using a Shamir system to encrypt this information, “The key shares were then distributed to multiple individuals through the [blind] trusts” and “he alone does not have ability to access the encrypted file and data contained in it.” *Id.*

The Court held a hearing on June 11 on the Motion. DE 221. Plaintiffs’ counsel pointed out that under oath in his deposition Dr. Wright denied ever putting bitcoin into a trust, and denied putting any private keys into the Tulip Trust. DE 221 at 8-9. After hearing further oral argument from the parties, the Court once again gave Dr. Wright an opportunity (and a deadline of June 17, 2019) to “produce a complete list of all bitcoin that he mined prior to December 31, 2013.” DE 217. Again, the Court did not order a list of public addresses. The Court simultaneously entered an Order to Show Cause why it should not certify a contempt of court to the District Judge. The Court also put Dr. Wright on notice that it was considering sanctions under Rule 37 for his

continued non-compliance with the Court's March 14 Order. DE 217 at 5; DE 221 at 32-33. An evidentiary hearing was scheduled for June 28.

Dr. Wright's deposition reconvened on June 28 immediately prior to the evidentiary hearing. I presided over the deposition to rule on any objections. Dr. Wright was asked about the trusts referenced in his declaration. He responded, "I'm not the trustee of these trusts." DE 270-2 at 7. Dr. Wright was asked if he transferred all of his bitcoin into blind trust in 2011. He responded, "What I actually did was, I transferred the algorithms and software that I had used, the nonpublic version of Bitcoin that I was working on, into an encrypted file. The encrypted file was then – basically the key was split so that other people could have it." DE 270-2 at 21-22.

THE EVIDENTIARY HEARING

The Court heard from three live witnesses during two days of testimony: Dr. Wright, Steven Coughlan a/k/a Steve Shadders, and Dr. Matthew Edman. DE 236, 264. Plaintiffs also submitted excerpts from the depositions of Jonathan Warren and Dr. Wright. DE 261, 270. The Court heard oral argument on August 26, 2019.

Dr. Wright testified to his inability to comply with the Court's Orders. He claimed that after drug dealers and human traffickers began using Bitcoin, he wanted to disassociate himself completely from it. He engaged David Kleiman for that purpose. As part of that process, Dr. Wright put control over the bitcoin he mined in 2009-2010 into an encrypted file, which he put into a blind trust called the Tulip Trust. The encryption key was divided into multiple key slices. A controlling number of the key slices were given to Mr. Kleiman, who distributed them to others through the trust. Today, Dr. Wright does not have access to a sufficient number of the key slices to decrypt the file. Therefore, he cannot produce a list of his bitcoin holdings.

Mr. Shadders testified to efforts he made to filter the public Bitcoin blockchain to identify Dr. Wright's bitcoin. Dr. Edman testified about alleged alterations to documents.

APPLICABLE LEGAL PRINCIPLES

The Court gave notice that it would consider discovery sanctions under Federal Rule of Civil Procedure 37, and independently consider sanctions for contempt.⁹

Rule 37

Rule 37 authorizes the Court to award attorney's fees against a party and/or the party's counsel as a sanction for certain discovery-related conduct. Additionally, the Court may impose sanctions that affect the further litigation of the merits (what I will call "substantive sanctions"), including:

- (i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;
- (ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;
- (iii) striking pleadings in whole or in part;
- (iv) staying further proceedings until the order is obeyed;
- (v) dismissing the action or proceeding in whole or in part;
- (vi) rendering a default judgment against the disobedient party; or
- (vii) treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

⁹ Plaintiffs' Motion for Sanctions also references the Court's inherent power to sanction for bad faith conduct. DE 210 at 5. The June 14 Order on Plaintiff's Motion to Compel did not put Dr. Wright on notice that the Court would consider sanctions under its inherent power. The sanctions otherwise available under Rule 37 are sufficient to address Dr. Wright's behavior, so the Court would not impose additional sanctions even if it were to invoke its inherent power.

Fed R. Civ. P. 37(b)(2)(A).

The burden of proof for Rule 37 sanctions is a preponderance of the evidence. *Ramirez v. T&H Lemont, Inc.*, 845 F.3d 772, 777 (7th Cir. 2016). Rule 37 sanctions “are intended to: (1) compensate the court and other parties for the added expense caused by discovery abuses; (2) compel discovery; (3) deter others from engaging in similar conduct; and (4) penalize the offending party or attorney.” *Steward v. Int'l Longshoreman's Ass'n., Local No. 1408*, 306 Fed. Appx. 527, 529 (11th Cir. 2009). District courts possess wide discretion over the discovery process and when discovery sanctions are appropriate. *Dude v. Cong. Plaza, LLC*, 17-80522-CIV, 2018 WL 4203888, at *5 (S.D. Fla. July 20, 2018) (J. Matthewman), *report and recommendation adopted sub nom. Dude v. Cong. Plaza, LLC*, 17-CV-80522, 2018 WL 4203886 (S.D. Fla. Aug. 29, 2018). “The severe sanctions permitted by Rule 37(b) are usually only imposed by district courts upon a finding ‘(1) that the party’s failure to comply with the order was willful or a result of bad faith, (2) the party seeking sanctions was prejudiced by the violation, and (3) a lesser sanction would fail to adequately punish and be inadequate to ensure compliance with court orders.’” *Id.* (citations omitted).

In a situation where a party asserts inability to comply with a discovery order, the proponent of sanctions bears the initial burden of making a *prima facie* showing that the opposing party failed to comply with the Court’s order. Once the moving party makes that showing, the opposing must introduce evidence that it was impossible to comply. *See Malautea v. Suzuki Motor Co.*, 987 F.2d 1536, 1542-43 (11th Cir. 1993) (affirming sanctions where non-movant had “shown no evidence of inability to comply”); *Broadcast Music, Inc. v. Bourbon Street Station, Inc.*, 2010 WL 1141584, *2 (M.D. Fla. Mar. 23, 2010); *Chairs v. Burgess*, 143 F.3d 1432, 1436 (11th Cir. 1998) (quoting *Citronelle-Mobile Gathering, Inc. v. Watkins*, 943 F.2d 1297, 1301 (11th Cir. 1991)). That is, the

party must establish that he “has in good faith employed the utmost diligence in discharging his ... responsibilities.” *Phoenix Marine Enterprises, Inc. v. One (1) Hylas 46' Convertible Sportfisherman Hull No. 1*, 681 F. Supp. 1523, 1528–29 (S.D. Fla. 1988) (J. Nesbitt) (quoting *Natural Resources Defense Council, Inc. v. Train*, 510 F.2d 692, 713 (D.C. Cir. 1975)); *Piambino v. Bestline Prod., Inc.*, 645 F. Supp. 1210, 1214 (S.D. Fla. 1986).

This burden is satisfied by making “in good faith *all* reasonable efforts to comply.” *United States v. Rizzo*, 539 F.2d 458, 465 (5th Cir. 1976). We construe this requirement strictly. “Even if the efforts he did make were ‘substantial,’ ‘diligent’ or ‘in good faith,’ ... the fact that he did not make ‘all reasonable efforts’ establishes that [respondent] did not sufficiently rebut the ... prima facie showing of contempt. The ... use of a ‘some effort’ standard for measuring the strength of [the] defense [would be] an abuse of discretion.”

Id. at 1213 (quoting *United States v. Hayes*, 722 F.2d 723, 725 (11th Cir.1984)).¹⁰

Several provisions of the Federal Rules of Civil Procedure authorize reasonable expenses, including attorney’s fees, as a sanction for discovery violations. *See* Fed. R. Civ. P. 37(a)(5)(A) (expenses associated with motion to compel); Fed. R. Civ. P. 37(b)(2)(C) (expenses associated with failure to comply with discovery order); Fed. R. Civ. P. 26(c)(3) (expenses associated with motion for protective order); Fed. R. Civ. P. 26(g)(3) (expenses associated with non-compliance with discovery certification). Rule 37(a)(5) authorizes an award of expenses if a Motion to Compel is granted after a party “fails to produce documents . . . as requested under Rule 34.” Fed. R. Civ. P. 37(a)(3)(iv). “[A]n evasive or incomplete disclosure, answer, or response must be treated as a failure to disclose, answer, or respond.” Fed. R. Civ. P. 37(a)(4). All of these rules apply the same structure: the prevailing party receives reasonable expenses, including attorney’s fees, unless the

¹⁰ Many of the cases addressing inability to comply involve contempt proceedings, not Rule 37 sanctions. Nevertheless, the situations are analogous and I will apply the same burden-shifting approach.

losing party's conduct was "substantially justified" and/or "other circumstances make an award of expenses unjust."

Contempt

Where, as here, the parties have not consented to have a United States Magistrate Judge preside over this civil case, I cannot hold a person in civil contempt or indirect criminal contempt (i.e., a contempt occurring outside the Court's presence). 28 U.S.C. § 636(e)(6)(B). Instead, if the person's conduct, "in the opinion of the magistrate judge," constitutes an indirect criminal contempt or a civil contempt, "the magistrate judge shall forthwith certify the facts to a district judge" for further proceedings. *Id.*

The sanction of civil contempt "may be employed for either or both of two purposes: to coerce the defendant into compliance with the court's order, and to compensate the complainant for losses sustained." *Local 28 of Sheet Metal Workers' Int'l Ass'n v. EEOC*, 478 U.S. 421, 443 (1986) (internal quotation marks omitted), *cited and quoted in F.T.C. v. Leshin*, 719 F.3d 1227, 1231 (11th Cir. 2013). "A finding of civil contempt must be supported by clear and convincing evidence . . . The evidence must establish that: (1) the allegedly violated order was valid and lawful; (2) the order was clear and unambiguous; and (3) the alleged violator had the ability to comply with the order. The absence of willfulness is not a defense to a charge of civil contempt, and substantial, diligent, or good faith efforts are not enough; the only issue is compliance." *Jysk Bed'N Linen v. Dutta-Roy*, 714 Fed. Appx. 920, 922 (11th Cir. 2017) (citations omitted). Clear and convincing evidence is evidence that "place[s] in the mind of the ultimate factfinder an abiding conviction that the truth of its factual contentions is 'highly probable.'" *Colorado v. New Mexico*, 467 U.S. 310, 316 (1984); *Powell v. Home Depot U.S.A.*, 2009 WL 1515073, at *8 (S.D. Fla. June 1, 2009) (J. Hurley).

Criminal contempt is punitive. An alleged criminal contempt occurring outside the presence of the Court (i.e., an indirect contempt) must be proven beyond a reasonable doubt. *Int'l Union, United Mine Workers of Am. v. Bagwell*, 512 U.S. 821, 834 (1994).

FINDINGS

I make the following findings, each of which will be further explained below. First, I find that Dr. Wright has not met his burden of proving by a preponderance of the evidence that he is unable to comply with the Court's Orders. Second, in my opinion the evidence in the record before me does not rise to the level of proof beyond a reasonable doubt necessary for a criminal contempt. Although I find clear and convincing evidence that would support a civil contempt, the sanctions available under Rule 37 are sufficient, so I exercise my discretion and do not certify facts to Judge Bloom for civil contempt proceedings. Third, an award of attorney's fees is warranted against Dr. Wright, but not against his counsel. Fourth, I impose the following sanctions pursuant to Rule 37(b). For purposes of this action, it is established that (1) Dr. Wright and David Kleiman entered into a 50/50 partnership to develop Bitcoin intellectual property and to mine bitcoin; (2) any Bitcoin-related intellectual property developed by Dr. Wright prior to David Kleiman's death was property of the partnership, (3) all bitcoin mined by Dr. Wright prior to David Kleiman's death ("the partnership's bitcoin") was property of the partnership when mined; and (4) Plaintiffs presently retain an ownership interest in the partnership's bitcoin, and any assets traceable to them. To conform to these established facts, the Court strikes Dr. Wright's Third Affirmative Defense (Good Faith), Fourth Affirmative Defense (Accord and Satisfaction), Fifth Affirmative Defense (Release), Sixth Affirmative Defense (Payment), Seventh Affirmative Defense (Set-off), Eighth Affirmative Defense (Failure to Mitigate Damages), Seventh [sic] Affirmative Defense (Waiver), and Tenth Affirmative Defense (Statute of Frauds).

DISCUSSION

The factual issue for decision is whether a preponderance of the evidence proves that Dr. Wright is incapable of complying with the Court's Orders, specifically, whether Dr. Wright proved that the evidence necessary to identify his bitcoin holdings on December 31, 2013, is encrypted in a file that is in a blind trust and for which Dr. Wright does not have (and cannot presently get) the decryption keys. The evidence offered in support of this hypothesis was (1) the testimony of Dr. Wright and (2) the testimony of Steven Coughlan a/k/a Steve Shadders.

A finder of fact must consider the following questions in assessing witness credibility:

1. Did the witness impress you as one who was telling the truth?
2. Did the witness have any particular reason not to tell the truth?
3. Did the witness have a personal interest in the outcome of the case?
4. Did the witness seem to have a good memory?
5. Did the witness have the opportunity and ability to accurately observe the things he or she testified about?
6. Did the witness appear to understand the questions clearly and answer them directly?
7. Did the witness's testimony differ from other testimony or other evidence?

Eleventh Circuit Pattern Civil Jury Instruction 3.4. As will be discussed below, the evidence in the record demonstrated that Dr. Wright (directly and through counsel) made inconsistent statements about material matters. In considering that evidence, the Court is mindful "that a simple mistake doesn't mean a witness wasn't telling the truth as he or she remembers it. People naturally tend to forget some things or remember them inaccurately. So, if a witness misstated something, you must decide whether it was because of an innocent lapse in memory or an intentional deception. The significance of your decision may depend on whether the misstatement is about an

important fact or about an unimportant detail.” Eleventh Circuit Pattern Civil Jury Instruction 3.5.1. A party’s disbelieved testimony can be considered substantive evidence in support of the opposing party’s burden of proof. *United States v. Brown*, 53 F.3d 312, 314 (11th Cir. 1995) (“[A] statement by a defendant, if disbelieved by the jury, may be considered as *substantive evidence* of the defendant’s guilt.”) (emphasis in original).

Mr. Shadders testified that he was asked by Dr. Wright to try to reconstruct Dr. Wright’s bitcoin holdings by applying six data filters to the public Bitcoin blockchain. Mr. Shadders is the Chief Technology Officer at nChain, Ltd., a Bitcoin technology company in London. DE 264 at 12. Dr. Wright is the Chief Scientist at nChain. DE 236 at 5.

Dr. Wright provided the six filter criteria. Mr. Shadders wrote computer code to apply the criteria to the master blockchain. Mr. Shadders devoted approximately 12-16 hours total to the project. DE 264 at 49. His analysis identified approximately 27,000 bitcoin public addresses that met all six criteria. Because one of the criteria was that the public address correspond to a newly mined Bitcoin block, each public address represents 50 bitcoin. Therefore, Mr. Shadders’ analysis identified approximately 1,350,000 bitcoin. These could not be further distilled to identify bitcoin controlled by Dr. Wright.

I found Mr. Shadders’ testimony about his effort to apply filter criteria to the public blockchain to be credible and worthy of belief. I understand the inference that Dr. Wright would not have wasted Mr. Shadders’ time if Dr. Wright were capable of complying with the Court’s Orders. I also accept that Mr. Shadders’ efforts demonstrate a good faith attempt by Dr. Wright to comply. For the reasons discussed below, however, I give limited weight to these inferences.

I now turn to Dr. Wright’s testimony.

Apparently, dead men tell no tales, but they (perhaps) send bonded couriers. *See* John Dryden, “The Spanish Fryar or The Double Discovery”, Act IV, Scene 1 (1681) (“there is a Proverb, I confess, which says, That Dead men tell no Tales.”). I completely reject Dr. Wright’s testimony about the alleged Tulip Trust, the alleged encrypted file, and his alleged inability to identify his bitcoin holdings.

Dr. Wright’s story not only was not supported by other evidence in the record, it defies common sense and real-life experience. Consider his claims. He designed Bitcoin to be an anonymous digital cash system with an evidentiary trail. DE 236 at 15. He mined approximately 1,000,000 bitcoin, but there is no accessible evidentiary trail for the vast majority of them. He is a latter-day Dr. Frankenstein whose creation turned to evil when hijacked by drug dealers, human traffickers, and other criminals. *Id.* at 16-17. To save himself, he engaged David Kleiman to remove all traces of his involvement with Bitcoin from the public record. *Id.* at 16. As part of his efforts to disassociate from Bitcoin and “so that I wouldn’t be in trouble,” he put all his bitcoin (and/or the keys to it – his story changed) into a computer file that is encrypted with a hierarchical Shamir encryption protocol. *See Id.* at 23. He then put the encrypted file into a “blind” trust (of which he is one of the trustees), gave away a controlling number of the key slices to now-deceased David Kleiman, and therefore cannot now decrypt the file that controls access to the bitcoin. His only hope is that a bonded courier arrives on an unknown dated in January 2020 with the decryption keys. If the courier does not appear, Dr. Wright has lost his ability to access billions of dollars worth of bitcoin, and he does not care. *Id.* at 21-22. Inconceivable.

During his testimony, Dr. Wright’s demeanor did not impress me as someone who was telling the truth. When it was favorable to him, Dr. Wright appeared to have an excellent memory and a scrupulous attention to detail. Otherwise, Dr. Wright was belligerent and evasive. He did

not directly and clearly respond to questions. He quibbled about irrelevant technicalities. When confronted with evidence indicating that certain documents had been fabricated or altered, he became extremely defensive, tried to sidestep questioning, and ultimately made vague comments about his systems being hacked and others having access to his computers. None of these excuses were corroborated by other evidence.

Sadly, Dr. Wright does not write on a clean slate. As Judge Bloom recently noted in denying Dr. Wright's Motion for Judgment on the Pleadings, Dr. Wright has taken directly conflicting factual positions at different times during this litigation. DE 265 at 10 (“[T]he record is replete with instances in which the Defendant has proffered conflicting sworn testimony before this Court.”). As discussed below, that behavior continued before me.

Dr. Wright has a substantial stake in the outcome of the case. If Plaintiffs succeed on their claims, Dr. Wright stands to lose billions of dollars. That gives him a powerful motive not to identify his bitcoin. As long as the relevant addresses remain secret, he can transfer the bitcoin without the Plaintiffs being able to find them. After all, Bitcoin is an anonymous cybercurrency.

Similarly, Dr. Wright had many reasons not to tell the truth. Most notably, Dr. Wright might want to prevent the Plaintiffs (or others) from finding his Bitcoin trove. Alternatively, there was evidence indicating that relevant documents were altered in or about 2014, when the Australian Tax Office was investigating one of Dr. Wright's companies. Perhaps Dr. Wright's testimony here is motivated by certain legal and factual positions he took in the Australian Tax Office investigation and from which he cannot now recede.

There was substantial credible evidence that documents produced by Dr. Wright to support his position in this litigation are fraudulent. There was credible and compelling evidence that documents had been altered. Other documents are contradicted by Dr. Wright's testimony or

declaration. While it is true that there was no direct evidence that Dr. Wright was responsible for alterations or falsification of documents, there is no evidence before the Court that anyone else had a motive to falsify them. As such, there is a strong, and un rebutted, circumstantial inference that Dr. Wright willfully created the fraudulent documents.

One example is the Deed of Trust document for the Tulip Trust. Among the trust assets identified in the purported Deed of Trust creating the Tulip Trust on October 23, 2012, are “All Bitcoin and associated ledger assets transferred into Tulip Trading Ltd by Mr David Kleiman on Friday, 10th June 2011 following transfer to Mr Kleiman by Dr Wright on the 09th June 2011 . . . This incles [sic] the 1,200,111 Bitcoin held under the former arrangement and the attached conditions.” P. Ex. 9 at 2. Notably absent from the list of trust assets is any encrypted file, software, public or private keys. The Deed of Trust states that the parties forming the Tulip Trust are Wright International Investments Ltd and Tulip Trading Ltd. *Id.* at 1. There was credible and conclusive evidence at the hearing that Dr. Wright did not control Tulip Trading Ltd. until 2014. P. Exs. 11-14; DE 236 at 88-96. Moreover, computer forensic analysis indicated that the Deed of Trust presented to the Court was backdated. The totality of the evidence in the record does not substantiate that the Tulip Trust exists. Combining these facts with my observations of Dr. Wright’s demeanor during his testimony, I find that Dr. Wright’s testimony that this Trust exists was intentionally false.¹¹

Dr. Wright’s false testimony about the Tulip Trust was part of a sustained and concerted effort to impede discovery into his bitcoin holdings. Start with Dr. Wright’s deceptive and incomplete discovery pleadings. He testified at the evidentiary hearing that at least as early as

¹¹ Although I am only required to make this finding by a preponderance of the evidence, I find clear and convincing evidence to support it.

December 2018 he knew that he could not provide a listing of his bitcoin holdings. Yet, the Court was not told this “fact” until April 18, 2019. I give Dr. Wright the benefit of the doubt that prior to May 14 the Plaintiffs were seeking information that went beyond a list of his bitcoin holdings on December 31, 2013. After the May 14 discovery hearing, however, Dr. Wright was aware that the Court expected him to provide Plaintiffs with sufficient information so those bitcoin holdings could be traced.

Nevertheless, having failed to hold off discovery on legal grounds, after March 14, Dr. Wright changed course and started making affirmative misleading factual statements to the Court. His April 18 Motion argued for the first time, “In 2011, Dr. Wright transferred ownership of all his Bitcoin into a blind trust. Dr. Wright is not a trustee or beneficiary of the blind trust. Nor does Dr. Wright know any of the public addresses which hold any of the bitcoin in the blind trust. Thus, Dr. Wright, does not know and cannot provide any other public addresses.” This pleading was intended to communicate the impression that Dr. Wright had no remaining connection to the bitcoin. It was also intended to create the impression that the bitcoin themselves had been transferred to the trust.¹²

Dr. Wright almost immediately made irreconcilable statements about the Tulip Trust. The April 18 Motion stated it was a blind trust and he was not a trustee. His sworn declaration three weeks later stated that he is one of the trustees of the Tulip Trust. The trust can hardly be considered “blind” (as represented in the April 18 Motion) if Dr. Wright is one of the trustees. At

¹² Although the pleading was not verified, it was signed by Dr. Wright’s counsel. By signing the document, they certified that “the allegations and other factual contentions [in the pleading had] evidentiary support.” Fed. R. Civ. P. 11. The sole source for that evidentiary support would have been Dr. Wright, so the Court finds that he provided the information contained in the April 18 Motion.

least one set of these representations about the trust and Dr. Wright's status as a trustee necessarily is intentionally misleading.

Dr. Wright also changed his story about what is in the alleged trust. The April 18 Motion states that Dr. Wright's *bitcoin* had been transferred to a blind trust, and therefore are owned by the trusts, not by Dr. Wright. The Court gave Dr. Wright an extension of time so he could meet with his counsel to draft and file a declaration about the trust. In the May 8 declaration, he swore that he met with counsel and that he provided counsel "with additional details and clarity regarding trusts that I settled that *hold or held Bitcoin* that I mined or acquired on or before December 31, 2013." DE 222 at ¶ 3 (emphasis added). He further swore, "In June 2011, I took steps to consolidate the Bitcoin I mined with Bitcoin that I acquired and other assets. In October 2012, a formal trust document was executed, creating a trust *whose corpus included the Bitcoin that I mined, acquired and would acquire* in the future. The name of that trust is Tulip Trust. It was formed in the Seycelles [sic]." *Id.* at ¶ 5 (emphasis added). His declaration was unequivocal that the trust held bitcoin. Nevertheless, at his deposition on June 26 (and at the evidentiary hearing), he changed his story to say that the trust contained an encrypted file with the keys to the bitcoin, not the bitcoin itself.

The hearing testimony that the trust holds only keys, not bitcoin, cannot be reconciled with the statements in the April 18 Motion and the May 8 declaration that it contains bitcoin. At least one of these representations is intentionally false. During his testimony at the evidentiary hearing, Dr. Wright made a point of being precise in his use of terms, including contesting whether a document was an email or a pdf of an email. It is not credible that, given his claim to have an unmatched understanding of Bitcoin, he would have mistaken the Bitcoin currency for the keys that control the ability to transfer the currency. I find instead that he belatedly realized that any

transaction(s) transferring bitcoin into the alleged Tulip Trust would be reflected on the Bitcoin master blockchain, that he would then be required to identify those transaction(s), and that Plaintiffs could use that information to trace the bitcoin. So, Dr. Wright changed his story to say that only the keys had been transferred.

Ultimately, Dr. Wright's claim of inability to comply with the Court's Orders relies on the existence of an encrypted file in the Tulip Trust containing the information necessary to reconstruct Dr. Wright's bitcoin holdings. I find that this file does not exist. Dr. Wright testified this file is an encrypted compressed file containing multiple sub-files. He swore, "Each of those files has a differently calculated encryption key . . . It's a hierarchical system, where, based on a combination of the file hash and the original encryption key – there are a variety of those – there are multiple Shamir schemes." DE 236 at 107. The Shamir scheme divides a single encryption key into multiple key slices; some subset of the total key slices is needed to decrypt the file.¹³ Dr. Wright testified that 15 key slices existed for the outermost file, only eight key slices were needed to decrypt this file, but he only had access to seven key slices. DE 236 at 125-26; *see also* DE 236 at 114 ("The eight of 15 is the key that we're talking about to regenerate all of the addresses"). After observing Dr. Wright's demeanor and the lack of any other credible evidence in the record that this file exists, I find that a preponderance of the evidence establishes that no such file exists and that Dr. Wright's testimony was intentionally false.¹⁴

¹³ For a more detailed discussion of the Shamir scheme see this Court's Order on Plaintiff's Motion to Compel, DE 217, and Appendix 1 to this Order.

¹⁴ Here, too, although the necessary burden of proof is a preponderance of the evidence, there was clear and convincing evidence to support this finding. One other point. Dr. Wright testified that the key slices had to be applied in a particular order. DE 236 at 108, 125-26. This testimony is inconsistent with Dr. Shamir's paper describing his encryption scheme. *See* Adi Shamir, How to Share a Secret, Communications of the ACM, Vol 22, No. 11, Nov. 1979, at 612. According to the paper, a Shamir Scheme is decrypted by inserting each key slice into the same polynomial to

Another aspect of Dr. Wright's story also changed at the evidentiary hearing. He argued for the first time that a list of public addresses was meaningless. This position is particularly disturbing because it was Dr. Wright who first injected the idea of public addresses into this discovery matter. At the May 14 hearing, Dr. Wright's counsel first introduced the idea of compiling a list of his Bitcoin holdings by using public addresses. Admittedly, counsel answered the Court's question without consulting with Dr. Wright and without time to fully research the situation. If, as Dr. Wright now asserts, counsel was wrong, Dr. Wright (the self-proclaimed creator of Bitcoin and therefore a person who claims to have intimate knowledge of how Bitcoin works) should have corrected the record long before the evidentiary hearing. Instead, in his April 18 motion, Dr. Wright explained why he could not produce a list of public addresses. He never said that public addresses lacked evidentiary value. This behavior continued in Dr. Wright's May 8 declaration, where he again talked about public addresses, but never argued that they were meaningless.

Although Dr. Wright may not have an obligation to correct an opposing party if its discovery request is imprecise, the Court is different, particularly where (as here) the Court's intent was unmistakable. It was clear that the Court was ordering Dr. Wright to produce evidence to document the existence and extent of his bitcoin holdings, so that Plaintiffs could attempt to trace them through the master blockchain. If, as Dr. Wright now claims, the public addresses are not the proper data point to identify the bitcoin he held on December 31, 2013, he had an obligation

create a series of linear equations. These equations are then solved simultaneously. There is no ordering of the key slices. *See* Exhibit 1. That being said, I do not exclude the possibility that Dr. Wright could have employed a modified Shamir Scheme, so I do not consider this testimony in making my findings.

to tell the Court. Either his delay in to doing so is deceptive and misleading, or his testimony that the public address is a meaningless piece of evidence is intentionally false.

In sum, after days of testimony, multiple discovery hearings, and lengthy pleadings, the sole evidence supporting Dr. Wright's claim that he cannot comply with the Court's Orders is the uncorroborated word of Dr. Wright. That word is insufficient to meet his evidentiary burden. Moreover, the totality of the evidence, including a negative inference drawn from Dr. Wright's incredible testimony and use of fraudulent documents, is more than sufficient to meet Plaintiffs' burden.

Dr. Wright argues that he would never risk going to jail for contempt or having sanctions imposed against him if he could produce a list of his bitcoin holdings. He argues it would not be credible that anyone would make that choice. Equally, if not more incredible, is the idea that someone who controlled almost 1 million bitcoin would encrypt it in a way that he could not access it, and then would not care if he lost it all. Additionally, as discussed above, there are many reasons a person in Dr. Wright's situation would take that risk.

REMEDY

I now turn to the question of a proper remedy. Plaintiffs' Motion asked the Court to declare that "the 1,100,111 bitcoin referenced to in to [sic] the Tulip Trust document is joint property belonging equally to both Dave Kleiman and Craig Wright." DE 210 at 6. On August 26, at oral argument on the Motion, Plaintiffs asked the Court to strike Dr. Wright's pleadings. Rule 37 specifically recognizes that an appropriate discovery sanction is for the Court to deem certain facts established for purposes of this action. Fed. R. Civ. P. 37(b)(2)(a)(i). Rule 37 also permits a Court to strike pleadings. Fed. R. Civ. P. 37(b)(2)(A)(iii).

I find without hesitation that sanctions are not warranted against Dr. Wright's counsel. Several Rules of Civil Procedure authorize the Court to require a party's counsel to pay expenses associated with discovery violations; the expense award can be separately against counsel or jointly against counsel and the client. *See* Fed. R. Civ. P. 37(a)(5)(A), (B); Fed. R. Civ. P. 37(b)(2)(C); Fed. R. Civ. P. 26(g)(3). The Court finds no basis to sanction Dr. Wright's counsel. I have conducted numerous hearings and have been able to closely observe counsel's conduct. Counsel has zealously and ethically advocated for their client. Counsel has unfailingly been candid with this Court, even when Dr. Wright's conduct and conflicting statements have created awkward situations for counsel. I find that counsel reasonably relied on Dr. Wright as a source of information. I find that Dr. Wright, alone, is fully responsible for any evasion, incomplete or false representations to the Court, or non-compliance with the Court's orders.

There is clear and convincing evidence that Dr. Wright's non-compliance with the Court's Orders is willful and in bad faith, that Plaintiffs have been prejudiced, and (particularly given the extended pattern of non-compliance and its egregiousness) a lesser sanction is not adequate to punish or to ensure future compliance with the Court's Orders. Therefore, sanctions under Rule 37(b) are warranted.

To this day, Dr. Wright has not complied with the Court's orders compelling discovery on May 14 and June 14. Rather, as described above, the evidence establishes that he has engaged in a willful and bad faith pattern of obstructive behavior, including submitting incomplete or deceptive pleadings, filing a false declaration, knowingly producing a fraudulent trust document, and giving perjurious testimony at the evidentiary hearing. Dr. Wright's conduct has prevented Plaintiffs from obtaining evidence that the Court found relevant to Plaintiffs' claim that Dr. Wright and David Kleiman formed a partnership to develop Bitcoin technology and to mine bitcoin.

Plaintiffs have also been prejudiced by not being able to try to trace the bitcoin that was mined. His conduct has wasted substantial amounts of the Court's and the Plaintiffs' time and resources. It has unnecessarily protracted this litigation.

Counsel for Dr. Wright argued that it would be fundamentally unfair to Dr. Wright, and contrary to concepts of justice to impose discovery sanctions that forfeited his right to fully litigate the merits of his case. I have found that Dr. Wright intentionally submitted fraudulent documents to the Court, obstructed a judicial proceeding, and gave perjurious testimony. No conduct is more antithetical to the administration of justice. The sanctions I am imposing are necessary to achieve the remedial and punitive purposes of Rule 37. No lesser sanction would suffice.

WHEREFORE, it is ordered that:

1. The Motion to Compel [DE 210] is GRANTED. The Court will consider an award of reasonable expenses, including attorney's fees, related to filing and litigating this motion. *See* Fed. R. Civ. P. 37(a)(5)(A).
2. The Court will consider an award of reasonable expenses, including attorney's fees, related to filing and litigating Dr. Wright's Motion Regarding Production of a List of the Public Addresses of his Bitcoin as of December 31, 2013 [DE 155], which the Court construes as a Motion for Protective Order. *See* Fed. R. Civ. P. 26(c)(3).
3. On or before **September 20, 2019**, Plaintiffs may submit a request for reasonable fees and costs. A Response and Reply may be filed in accordance with time frames in the Local Rules. The parties should indicate in their respective pleadings whether they believe an evidentiary hearing is needed.
4. Pursuant to Fed. R. Civ. P. 37(b)(2)(A)(i), the Court deems the following facts to be established for purposes of this action: (1) Dr. Wright and David Kleiman entered into

- a 50/50 partnership to develop Bitcoin intellectual property and to mine bitcoin; (2) any Bitcoin-related intellectual property developed by Dr. Wright prior to David Kleiman's death was property of the partnership, (3) all bitcoin mined by Dr. Wright prior to David Kleiman's death ("the partnership's bitcoin") was property of the partnership when mined; and (4) Plaintiffs presently retain an ownership interest in the partnership's bitcoin, and any assets traceable to them.
5. Pursuant to Fed. R. Civ. P. 37(b)(2)(A)(ii) and (iii), the Court strikes Dr. Wright's Third Affirmative Defense (Good Faith), Fourth Affirmative Defense (Accord and Satisfaction), Fifth Affirmative Defense (Release), Sixth Affirmative Defense (Payment), Seventh Affirmative Defense (Set-off), Eighth Affirmative Defense (Failure to Mitigate Damages), Seventh [sic] Affirmative Defense (Waiver), and Tenth Affirmative Defense (Statute of Frauds).

DONE AND ORDERED in Chambers this 27th day of August, 2019, at West Palm Beach in the Southern District of Florida.



BRUCE REINHART
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 18-CIV-80176-Bloom/Reinhart

IRA KLEIMAN, as personal representative of
the estate of David Kleiman, and
W&K INFO DEFENSE RESEARCH, LLC,

Plaintiffs,

v.

CRAIG WRIGHT,

Defendant.

_____ /

Appendix to Opinion

Shamir's (n,k) threshold scheme is based on the mathematical concepts of polynomial interpolation and modular arithmetic.¹ A polynomial equation is a function in one variable (here, the variable is x) with the following form:

$$f(x)=a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_kx^k$$

The largest power of x (here, k) is the “degree” of the polynomial. A polynomial function in one variable can be plotted as a curve in a two-dimensional coordinate plane. For example, a polynomial function of degree 1 plots as a straight line. A polynomial function of degree 2 (also known as a quadratic function) plots as a parabola. The precise shape of the curve depends on the coefficients assigned to the powers of x (that is, the values for a_0 , a_1 , a_2 , etc.). Polynomial interpolation is the technique of computing these coefficients so that the curve passes through a known set of points in a plane.²

Modular arithmetic, sometimes known as “clock arithmetic,” can be thought of as the mathematics of remainders.³ For example, on a clock, the only numbers that represent the hours of the day are 1-12. After the 12th hour of the day, we restart the count with the number 1 (which is the remainder after deducting 12 from 13). No number greater than 12 exists in this system. In mathematical terms, the number that comes after 12 is not 13 (because 13 does not exist); it is “1

¹ Adi Shamir, How to Share a Secret, Communications of the ACM, Vol 22, No. 11 (November 1979), p. 613.

² MIT OpenCourseWare. Lecture notes to Chapter 3 of Numerical Analysis (Course 18.330), p.1 (“Interpolation is the problem of fitting a smooth curve through a given set of points, generally as the graph of a function.”). https://ocw.mit.edu/courses/mathematics/18-330-introduction-to-numerical-analysis-spring-2012/lecture-notes/MIT18_330S12_Chapter3.pdf.

³ <https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/what-is-modular-arithmetic>.

modulo 12” (abbreviated “1 mod 12”). This pattern repeats. So, the numbers that would otherwise correspond to 25, 37, 49, 61 etc. are all equivalent to 1 mod 12.

Shamir’s (n,k) threshold scheme allows a person to use polynomial interpolation to encrypt a number in a way that can only be decrypted by simultaneously using multiple keys. The number of keys necessary for decryption is one more than the degree of the underlying polynomial. Therefore, for a linear function (degree 1), two keys are necessary. For a quadratic polynomial (degree 2), three keys are necessary.

So, to require k keys, start with a polynomial of order $k-1$. Then, select a finite field of prime order p , where p is greater than k and greater than the secret number you are trying to hide.⁴ Here’s an example. Use the quadratic polynomial $f(x)= a_0 + a_1x + a_2x^2$ over the finite field consisting of the integers less than or equal to 4 – $\{0,1,2,3,4\}$. This field is denoted F_5 .

- (1) Set a_0 equal to the number you want to hide. Here, we will designate “3” as the hidden data.
- (2) Assign an integer coefficient of your choice from the finite field to each of the other “ a ” terms of the polynomial. We assign $a_1=2$ and $a_2=1$, which gives the polynomial function: $f(x)= 3 + 2x + x^2$
- (3) Compute $f(x)$ for at least k values of x , where x is not equal to zero:

Ex:	for $x=1$	$f(x)=6$, which is 1 mod 5
	for $x=2$	$f(x)=11$, which is 1 mod 5
	for $x=3$	$f(x)=18$, which is also 3 mod 5
	for $x=4$	$f(x)=27$, which is 2 mod 5

- (4) Designate the ordered pairs corresponding to $(x, f(x))$:

(1, 1)	ie., when $x=1$, $f(x)$ is 1 mod 5
(2, 1)	ie., when $x=2$, $f(x)$ is 1 mod 5

⁴ A finite field is a type of algebraic structure. The number of elements of the field is its “order.” The order of a finite field must be a prime number or a power of a prime (usually represented as p). Michael Artin, *Algebra*, 1st Ed. (1991) p. 510, theorem 6.4.

- (3, 3) ie., when $x=3$, $f(x)$ is 3 mod 5
 (4, 2) ie., when $x=4$, $f(x)$ is 2 mod 5

The ordered pairs (1, 1), (2,1), (3,3), and (4,2) are the decryption keys. Anyone who has 3 or more of these keys can compute the hidden value of a_0 by plugging in the values of x and $f(x)$, then solving the simultaneous equations:

For (1,1), the polynomial becomes: $1 = a_0 + a_1 + a_2$

For (3,3), the polynomial becomes: $3 = a_0 + 3a_1 + 9a_2$ which is equivalent to $3 = a_0 + 3a_1 + 4a_2 \pmod{5}$

For (4,2), the polynomial becomes: $2 = a_0 + 4a_1 + 16a_2$, which is equivalent to $2 = a_0 + 4a_1 + a_2 \pmod{5}$

You now have three equations in three variables, which can be solved using simple linear algebra.⁵ The solution gives $a_0=3$, which is the number we wanted to encrypt.

⁵ See generally, Gilbert Strang, Introduction to Linear Algebra, 4th Edition, (2009), Chapter 2 (explaining how to solve a system of linear equations).