

SUPREME COURT OF THE STATE OF NEW YORK  
COUNTY OF NEW YORK: COMMERCIAL DIVISION PART 03M

-----X

PURSUIT CREDIT SPECIAL OPPORTUNITY FUND, L.P.,	<b>INDEX NO.</b>	<u>651070/2022</u>
Plaintiff,	<b>MOTION DATE</b>	<u>04/19/2023</u>
- v -	<b>MOTION SEQ. NO.</b>	<u>004</u>
KRUNCHCASH, LLC, KC PCRD FUND, LLC, JEFFREY HACKMAN, SEAN MCGHIE PLC	<b>DECISION + ORDER ON MOTION</b>	
Defendants.		

-----X

HON. JOEL M. COHEN:

The following e-filed documents, listed by NYSCEF document number (Motion 004) 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 133-1, 142-1, 143-1, 160, 161, 163, 166, 167, 168, 169, 170, 171, 172, 174, 175, 188, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 199-1, 200-1, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 268, 269, 270, 271, 272, 273, 271-1

were read on this motion for PROTECTIVE ORDER/DISCOVERY SANCTIONS.

This motion presents novel questions about litigation counsel’s obligations when she or he comes into possession, through non-party discovery, of a DropBox link that provides “live” access to an opposing party’s cloud-based corporate file directory.

In this case, Defendants subpoenaed documents from Plaintiff’s financial consultant. The resulting production contained several emails that included links to a DropBox site, which Plaintiff used effectively in lieu of an in-house server to store its electronic files. For approximately one week, Defendants’ counsel (and its client) accessed those links to download,

review, and analyze Plaintiff's *unproduced* electronic documents before notifying Plaintiff's counsel that it had done so.<sup>1</sup>

After completing its review, Defendants' counsel informed Plaintiff's counsel (by letter) that: (i) the DropBox links were "live"; (ii) all privileges with respect to the DropBox-linked documents purportedly had been waived by making the DropBox link available to Plaintiff's consultant; (iii) Defendants intended to use the files in an upcoming deposition; (iv) Defendants would make purportedly inculpatory (to Plaintiff) information gleaned from the files publicly available in court papers; and (v) demanded that Plaintiff dismiss this lawsuit with prejudice. Plaintiff promptly brought this issue to the Court's attention, seeking return of its confidential information and sanctions against Defendants and their counsel.

The parties have not cited (and the Court has not found) any precedent or guidance that directly addresses this vexing and concerning fact pattern. Nevertheless, the Court has little difficulty concluding that Defendants' counsel should have ceased reviewing the DropBox files as soon as they realized that they had obtained unauthorized access to Plaintiff's corporate file directory (as a practical matter, Pursuit's computer system) and should have ensured that their client did the same. At that point, it was no longer litigation discovery or "disclosure" within the meaning of the CPLR, inadvertent or otherwise, but something more akin to corporate espionage (albeit without the illicit break-in). Instead, counsel went on the offensive and threatened to use the information gleaned during its clandestine review for litigation advantage. Whether such review and use would have been permissible in the more common circumstance of receiving

---

<sup>1</sup> As noted below, Defendants' counsel represents that it refrained from reviewing a directory titled "Legal"; it is unclear whether counsel's client (who apparently began reviewing the documents before counsel became aware of what they contained) did so.

“inadvertent” production of individual privileged documents during the ordinary course of discovery is not before the Court. What makes this situation different, in the Court’s view, is that Plaintiff’s corporate file directory was not “produced” at all (although some of the documents contained *within* that directory ultimately were to be produced). Instead, the directory was surreptitiously and repeatedly *accessed* by counsel and their client under circumstances that should have raised professional alarm bells – loud ones.

The Court finds that Defendants should: (i) return all documents downloaded from the DropBox that were not independently produced by Plaintiff during discovery; (ii) certify destruction of all notes and other derivative work product reflecting the substance of such documents; and (iii) compensate Plaintiff for the cost (including attorneys’ fees) of this motion. Whether Defendant’s subsequent discovery requests will be curtailed on the ground that they were based on counsel’s improper review of the DropBox files—that is, fruit of the poisonous tree—will be addressed on a case-by-case basis.

### **Background Facts**

On or about September 9, 2022, Defendants KrunchCash, LLC, KC PCR Fund, LLC, Jeffrey Hackman, Sean McGhie PLC (collectively, “Defendants”) issued a subpoena to Ken Parzygnat (“Parzygnat”), Plaintiff Pursuit Credit Special Opportunity Fund, L.P.’s (“Plaintiff” or “Pursuit”) non-employee fund administrator, seeking various documents and communications concerning Parzygnat’s work for Pursuit as well as a deposition (NYSCEF 95). Parzygnat acted as Plaintiff’s paying agent, preparing financial statements and coordinating a financial review of its investments in 2019 (NYSCEF 156 [“Turner Aff.”] ¶¶ 7–8). On or about September 20, 2022, Plaintiffs issued its own subpoena to Parzygnat, seeking his communications with

Defendants, and preserving Plaintiff's right to question Parzygnat at his deposition (NYSCEF 96). No objections were made to Defendants' subpoena.

On November 3, 2022, Parzygnat submitted a production to both parties that included a single PDF file. The various emails included in the file contained approximately twenty DropBox links. DropBox Business is a cloud-based file storage and sharing service widely used by businesses as a file sharing and collaboration platform (NYSCEF 230 ¶ 23 ["Weiss Aff."]). DropBox allows a user to generate unique sharing links to documents or folders which are not publicly searchable (*id.* ¶33). Pursuit's principal testified that Pursuit does not maintain a private server separate and apart from DropBox (NYSCEF 195 at 12:6–9).

Parzygnat's production was uploaded to a shared drive maintained by Defendants' law firm and shared with Plaintiff's law firm (*see* NYSCEF 131 ¶¶ 15–16 ["Bea Aff."]). Plaintiff notified Defendants on November 4, 2022, that it was designating all documents produced by Parzygnat as "confidential." Defendant KrunchCash's principal, Jeffery Hackman ("Hackman"), testified that his counsel provided him with access to their shared drive which contained Parzygnat's production around November 4, 2022 (NYSCEF 219 ["Hackman Tr."] at 29:4-11) and that he downloaded a copy of the PDF to his desktop (Hackman Tr. at 29-31).

On November 7, 2022, Parzygnat uploaded additional documents, this time providing documents in a native Microsoft PST format (Bea Aff. ¶ 20). Hackman testified that he downloaded that production to his desktop as well (Hackman Tr. at 31). Later that same day, Plaintiff notified Defendants that it was provisionally designating all of the Parzygnat-produced documents as "attorney's eyes only" (or "AEO") (NYSCEF 134). On November 11, 2022, Plaintiff's counsel re-produced Parzygnat's documents to Defendants with bates stamps and confidentiality designations, indicating which documents warranted AEO or Confidential

treatment under the parties' Protective Order (Bea Aff. ¶ 24). There is no indication that Plaintiff's counsel was aware at this time that the documents contained links that provided real-time access to Pursuit's corporate file directory.

On November 14, 2022, after an extended review of the Pursuit's electronically stored corporate files accessed via the DropBox links, Defendants' counsel wrote a blunt letter to Pursuit's counsel regarding what they had discovered (NYSCEF 135). Counsel observed (“[a]s I’m sure you know”) that “Parzygnat’s production of a November 21, 2019 email from J. Scott Turner, and other similar emails, contain a live link to Pursuit’s DropBox,” and disclosed that “[t]he full contents of this DropBox are accessible to any party who clicks on the link.” For good measure, counsel added: “The link is still live.” Counsel maintained that by giving Parzygnat “unfettered access to Pursuit’s files maintained in DropBox” Pursuit had “waive[d] any attorney-client privilege of any document to which the third-party has access,” as “there is no reasonable expectation of privacy in a shared link in DropBox, as its own policies establish.” Counsel further argued that “[e]very single document in the DropBox currently is accessible to Mr. Parzygnat and responsive to our subpoena,” that “[a]fter careful study of the legal issues presented by Plaintiff’s haphazard disclosures, we have downloaded the contents of the DropBox and are entitled to use every document in it in this litigation,” and advised of their intent to use the documents in an upcoming deposition. Counsel went on to state that “the documents reveal” purportedly improper conduct by Pursuit which “gut[s] Pursuit’s case,” “establish[es] the fraudulent nature of the verification of Pursuit’s Amended Complaint,” and “give[s] rise to numerous, previously unknown counterclaims.” Counsel concluded by stating that “[a]ll these allegations will be made public” in court filings and “demand[ed] that Pursuit immediately dismiss its Verified Amended Complaint, with prejudice.”

Prior to receiving this letter, Plaintiff and its counsel were not aware of Defendants' access to Plaintiff's DropBox files or that those files were "live." The confidentiality of the DropBox-linked documents is not disputed. The collection included folders entitled "Legal," "Tax," and "Financials." Among other things, they included privileged documents, tax documents, personal identifying information of investors, and Pursuit's ESI collection at the direction of counsel of an entire email box. On November 21, 2022, Pursuit moved by Order to Show Cause requesting temporary and injunctive relief restraining and enjoining Defendants from accessing or using any and all documents obtained through its access to Pursuit's DropBox.

At the TRO hearing on November 21, 2022, counsel for Pursuit asserted "to a high degree of certainty" that Mr. Hackman viewed the DropBox files after November 7 (when the documents were designated as attorneys-eyes-only): "We actually triangulated this and compared the IP address to previous access points that Mr. Hackman had used . . . to a high degree of certainty it's Mr. Hackman" (NYSCEF 163 ["Nov 2022 Tr."] at 28:1-7). Pursuit also submitted to the Court an exhibit entitled "DropBox Activity Log -- Unknown Access Instances" (NYSCEF 139) showing "unknown" access from various cities, including Boca Raton, with a IP address 73.139xxx.xxx, which counsel believed to be Mr. Hackman (Nov 2022 Tr. at 8:18-21 ["The logs indicate a Boca Raton IP address that we had with the previous communication with Mr. Hackman, that demonstrates not just Mr. Berg and his team, it's Mr. Hackman that's been accessing them"])). Counsel for Pursuit explained that the "IP address and those reports generated directly from DropBox. I didn't create them myself. They are generated from the program. What they show are unknown access points. Only people who are unknown are the people who don't have the password and share access. So they are not Mr. Parzygnat." (Nov

2022 Tr. at 28:11-16). As discussed below, the evidence submitted in connection with this motion did not convincingly demonstrate these points.

Defendants' counsel represented at the hearing that "I opened the Legal file enough to learn that I shouldn't look at it. I stopped looking at them. But, Your Honor, the issue here is what did I do afterwards. I preserved the information and I let them know. Yes, it took a week because I'm very busy, but I let them know that" (Nov 2022 Tr. at 14:22-25; 15:1-2). Counsel further observed that "when I saw where I was, without waiving my work product privilege, believe me, I was incredibly careful about what I was doing" (*id.* at 16:4-6).

At the end of the November 21 hearing, the Court temporarily restrained and enjoined Defendants from accessing or using any and all documents or information accessed and/or obtained through the access of Dropbox folder (*id.* at 33:9-11), except as necessary to respond to the preliminary injunction motion (*id.* at 34-35). On November 22, 2023, the Court confirmed that ruling with a written order that "temporarily RESTRAINED and ENJOINED [Defendants] from accessing or using any and all documents or information accessed and/or obtained through the access of DropBox folders belonging to Plaintiff [and related entities], pending the hearing of this motion, provided, however, that Defendants' counsel may use previously accessed non-privileged documents solely to the extent reasonably necessary to respond to this motion" (NYSCEF 160). A hearing was set for January 20, 2023 (NYSCEF 160).

In December 2022, Plaintiff wrote to the Court alleging that the TRO had been violated because Defendant KrunchCash allegedly used documents accessed through Pursuit's DropBox in a related lawsuit in Florida (NYSCEF 166). KrunchCash denied these allegations (NYSCEF 171) and cross-moved for sanctions.

The parties engaged in targeted discovery with respect to the matters in dispute on this motion. Nevertheless, the record remains murky as to what happened between November 3, 2022, and November 14, 2022 with respect to Defendants' review and use of Pursuit's DropBox documents before and after the Court's TRO order. A brief overview follows.

At his deposition, KrunchCash's principal, Mr. Hackman, testified that he first accessed the DropBox links contained in Parzygnat's production on November 4 and realized that there were public links contained in the production which led him to Pursuit's entire DropBox (Hackman Tr. at 43:4-23). He testified that he "may" have had discussions with his attorney later in the day about this (*id.* at 44:8-15). He also testified that there were around twenty public links in Parzygnat's production, that he accessed Pursuit's DropBox more than once (Hackman Tr. at 50:13-25) and that he spent a couple hours each day for three days reviewing the files (Hackman Tr. at 57: 11-21). Hackman also testified that he downloaded the DropBox to his desktop (Hackman Tr. at 51-55), but that he did not have much time to review the downloads because he only downloaded it on November 7 (Hackman Tr. 57-58).

Hackman testified that when his attorney notified him that the Parzygnat production was designated "attorney's eyes only," he "stopped looking at it immediately" (Hackman Tr. at 33-34) and that later either on November 7 or the morning of November 8, the files were deleted from his desktop (*id.* at 34:9-18; *see also* Hackman Tr. at 79:15-18 ["Q Have you reviewed any documents that have a Bates stamp of attorneys' eyes' only after November 7th? A No"]).

Pursuit questioned Hackman as to whether he made any effort to determine his IP address, to which Hackman responded that "No, I didn't know that I had a duty to do so, but the answer would be no." (Hackman Tr. at 62-63). He provided his IP address and stated that it has not been altered or changed (Hackman Tr. at 64-65).



In response, Pursuit submitted the affidavit of a cybersecurity expert, Aaron Weiss (“Weiss”) of Forensic Recovery LLC, who had performed a forensic analysis of Pursuit’s DropBox environment and Defendants’ access (NYSCEF 230). Plaintiff argued that Weiss confirmed the purported “triangulation” analysis that showed Hackman repeatedly accessed Pursuit’s DropBox both before *and after* Parzygnat’s production was designated AEO under the Protective Order (Weiss Aff. ¶ 14(d), 49-65). However, when deposed, Pursuit’s expert could not verify that such “triangulation” evidence exists or that this analysis had occurred (NYSCEF 270 [“Weiss Tr.”] at 8:18-9:22 [Q: “Did you help triangulate Mr. Hackman's IP address prior to November 21, 2022? A: I don't know that -- I have not used the term "triangulate" in any of my work, no. Q: Alright. So, it's fair to say, is it not, that you had not done any work prior to that representation being made to the court by Ms. Bea on this matter? A: I don't believe so, but I would have to check -- check my records to see when work began after the agreement was signed.”] [Q: Is “triangulating an IP address” not a term of art in your business? A: I wouldn't say it's used to associate with IP address.”]; 76:22-77:7 [“Q. “Couldn’t the [] IP address be others in Boca Raton?” A. “If we were just looking at this sheet, I would say yes.”]).

As to the DropBox Activity Log, Mr. Weiss also testified that DropBox creates a spreadsheet of DropBox activity, but that he did not believe that DropBox uses the terms “unknown” or “known” (Weiss Tr. at 68:4-11 [“Q: And, using your expertise in computers, isn’t it true that the DropBox Activity Log makes no distinction between unknown access and known access, correct? THE WITNESS: I don't believe that it uses those terms, "unknown" or "known", in its recording, no.”] [objection omitted]), and thus, someone must have added that label to the spreadsheet (*id.* at 68:13-23 [“Q: And, so, somebody culled through the spreadsheet and labeled this document "Unknown Access Instances", right? THE WITNESS: Yes, somebody used that

language. I don't believe that's part of the spreadsheet that's downloaded.”] [objection omitted]).

Weiss further testified that he did not rely on the edited exhibit presented to this Court – only the original DropBox Activity Report (*id.* at 68:17-69:2 [“Q: And, do you rely on this document in any way, shape, or form in forming your opinions? A No. I used the original Activity Log.”]).

Mr. Weiss further testified that he did not confirm whether Parzygnat had accessed the DropBox from November 4 to November 14, which would have been relevant to determining whether the file access activity observed after November 7 might have been legitimate rather than continued review by Mr. Hackman (Weiss Tr. at 79:7-16 [Q: “Did you talk to Mr. Parzygnat to get his confirmation that he, A, reviewed Pursuit's DropBox from November 4 through November 14? A No. Q You didn't think that was important? A: I did not think it was important to speak with them, no.”] [objections omitted]).

## **DISCUSSION**

### **I. Pursuit’s Request for a Protective Order**

“The court may at any time on its own initiative, or on motion of any party or of any person from whom or about whom discovery is sought, make a protective order denying, limiting, conditioning or regulating the use of any disclosure device. Such order shall be designed to prevent unreasonable annoyance, expense, embarrassment, disadvantage, or other prejudice to any person or the courts” (CPLR 3103).

Pursuit’s motion for a protective order is granted in part. Although Plaintiff initially sought a protective order with respect to all documents and information obtained by Defendants through DropBox (NYSCEF 160), since that time Plaintiff confirmed that it has produced 92

percent of those same documents through discovery and the other 8 percent Defendants do not seek to use (NYSCEF 283 [“Tr. May 11, 2023”] at 81–82; 89:3-5).

Here, given Defendants’ unauthorized and undisclosed access to Pursuit’s live electronically stored corporate files, and the potential prejudice to Pursuit, the Court finds a protective order is warranted mandating the return of the DropBox documents that were not subsequently produced by Pursuit, as well as the destruction of any derivative materials (notes, etc.) relating to such documents. Since there was no opposition to this aspect of the motion, and because privilege has not been asserted with respect to the documents that have been independently produced, the Court need not decide whether Pursuit waived attorney-client privilege by sharing the DropBox link with Mr. Parzygnat.

## **II. Pursuit’s Request for Sanctions**

Pursuit seeks (i) sanctions against KrunchCash for violating the TRO and/or the Confidentiality Order by allowing Hackman to review the documents from the DropBox after it had been designated as attorney’s eyes only, and (ii) sanctions against KrunchCash counsel. Pursuit seeks an award of \$155,977, which represents Pursuit’s attorneys’ fees and costs in bringing this motion, and \$9,860 in fees relating to statutorily-required data breach notifications. Pursuit’s request for sanctions is granted in part.

The evidence currently available with respect to Mr. Hackman’s purported violation of the Confidentiality Order is equivocal. Hackman was permitted under the Order to review documents marked as “confidential,” and thus his admitted review of Pursuit documents prior to November 7 did not violate the Order. Hackman testified that when his attorney notified him that the Parzygnat production was designated “attorney’s eyes only,” he “stopped looking at it immediately” (Hackman Tr. at 33-34) and that later either on November 7 or the morning of

November 8, the files were deleted from his desktop (*id.* at 34:9-18, 79:15-18). Although the Weiss Affidavit (NYSCEF 230) provides some basis for inferring that an IP address associated with Mr. Hackman may have accessed Pursuit’s DropBox files after November 7, Mr. Weiss disclaimed during his deposition undertaking any “triangulation” analysis to confirm Hackman’s purported review of DropBox documents after November 7 (Weiss Tr. at 8:18-9:22; 76:22-77:7). He further testified that he did not confirm with Parzygnat as to whether he accessed the DropBox from November 4 to November 14 (Weiss Tr. at 79:7-16). At oral argument, Pursuit’s counsel acknowledged that in order to prove that Mr. Hackman accessed the DropBox after November 7, Pursuit would have to subpoena his ISP provider (NYSCEF 283, Tr. at 81:16-21), which it has not done. Thus, the evidentiary record at this stage is far from the “smoking gun” record Pursuit represented to the Court, and the Court thus cannot conclude based on the record presented, one way or another, whether Hackman accessed Pursuit’s DropBox after November 7, 2022. The Court declines, based on this record, to sanction Defendants for the purported violation of the Confidentiality Order or the TRO. That said, this decision does not preclude Pursuit from seeking additional information bearing on whether Defendants violated any applicable Court orders.

The record is sufficient, however, to assess Defendants’ and defense counsel’s initial and continued review of Pursuit’s DropBox documents, as well as their subsequent use of those materials. To begin with, the Court finds Defendants’ reliance on various “hyperlink” cases to be unpersuasive. Those cases by and large stand for the unremarkable proposition that when an email references a specific document by hyperlink rather than by a physical attachment, the producing party may be obligated to provide the linked document to ensure that the email communication is produced in complete form (*see e.g., IQVIA, INC. v Veeva Sys., Inc.*, 2:17-CV-

00177-CCC-MF, 2019 WL 3069203, at \*5 [DNJ July 11, 2019]; *Kelly v Provident Life and Acc. Ins. Co.*, 04-CV-0807-WQH (JMA), 2009 WL 10664172, at \*5 [SD Cal May 29, 2009]; *In re Telxon Corp. Sec. Litig.*, 1:01CV1078, 2004 WL 3192729, at \*24 [ND Ohio July 16, 2004]; *Shenwick v Twitter, Inc.*, 16-CV-05314-JST (SK), 2018 WL 5735176, at \*1 [ND Cal Sept. 17, 2018]). That is not what happened here. Those cases do not stand for the proposition that when an e-mail contains a link to an entire cloud-based file directory to facilitate the recipient's provision of services (*i.e.*, not as a link to specific documents referenced in the email), that automatically means that the producing party's entire cloud-based file directory becomes fair game for discovery. The implications of such a rule could be staggering and, in the Court's view, is not what CPLR Article 31 envisions.

As noted above, the Court has not found or been directed to guidance covering the precise fact pattern presented in this case – counsel using a hyperlink that permits unauthorized review of a litigation adversary's live electronically-stored corporate files. Rule 4.4 of the New York Rules of Professional Conduct addresses the more common fact pattern of inadvertent production of documents during discovery. The Rule provides that:

A lawyer who receives a document, electronically stored information, or other writing relating to the representation of the lawyer's client and knows or reasonably should know that it was inadvertently sent shall promptly notify the sender.

(Rules of Professional Conduct [22 NYCRR 1200.0] rule 4.4[b]). The comments to Rule 4.4 provide, in relevant part, that:

[2] . . . this Rule requires only that the receiving lawyer promptly notify the sender in order to permit that person to take protective measures. Although this Rule does not require that the receiving lawyer refrain from reading or continuing to read the document, a lawyer who reads or continues to read a document that contains privileged or confidential information may be subject to court-imposed sanctions . . . . Whether the lawyer or law firm is required to take additional steps,

such as returning the document or other writing, is a matter of law beyond the scope of these Rules, as is the question whether the privileged status of a document or other writing has been waived . . . .

[3] . . . substantive law or procedural rules may require a lawyer to refrain from reading an inadvertently sent document or other writing, or to return the document or other writing to the sender or permanently delete electronically stored information, or both. Accordingly, in deciding whether to retain or use an inadvertently received document or other writing, some lawyers may take into account whether the attorney-client privilege would attach. But if applicable law or rules do not address the situation, decisions to refrain from reading such a document or other writing or instead to return them, or both, are matters of professional judgment reserved to the lawyer. *See* Rules 1.2, 1.4.

(Rules of Professional Conduct [22 NYCRR 1200.0] rule 4.4[b]; Comment [2], [3]).

This Rule does not, in the Court's view, support Defendants' argument that its counsel was permitted to remotely download and review Pursuit's electronically stored corporate files prior to notifying Pursuit's counsel. Putting aside that continued review could present risks even in the more commonplace circumstances covered by Rule 4.4, here counsel was on much more fraught ground. It should have been apparent to counsel that repeatedly accessing Pursuit's live files via a DropBox link was outside the scope of the discovery process. As noted above, the majority of these documents were not *produced* to Defendants at that time, and certainly the directory itself was never produced. Even crediting the point that Pursuit should have exercised greater caution in securing its DropBox files, that does not provide a license for opposing counsel to conduct an unauthorized remote search of Pursuit's active electronically stored corporate files. In those circumstances, counsel should have notified opposing counsel and/or sought guidance from the Court as to what, if any, use could legitimately be made of the documents to which counsel had obtained access via the DropBox links.

The case law cited by the parties, while not directly on point, supports this conclusion. In *Lupin v Bender* (84 NY2d 562 [1994]), the plaintiff essentially stole a pile of defendant's

privileged documents that had been left in front of her during a court hearing, and provided them to her counsel who initially declined to read them but ultimately did so and presented them to defendant's counsel to gain leverage at a settlement conference. The trial court (Moskowitz, J.) dismissed the case under CPLR 3103. The Appellate Division affirmed, noting that “[plaintiff’s] improper conduct was ... compounded by counsel, who could have readily returned the documents or sought further direction from the court, rather than permitting his client to return to his office and make copies of the disputed documents and then sought to take advantage of such improper conduct by scheduling a ‘settlement conference’” (193 AD2d at 427-28). The Court of Appeals agreed, finding “ample support for the affirmed factual findings of wrongdoing by plaintiff, wholly apart from the conduct of her attorney that indisputably compounded it” (84 NY2d at 569). While the facts of the instant case are less egregious than in *Lupin* (there was no theft of privileged documents here, and striking of pleadings has not been suggested), counsel’s attempt to use documents obtained through an unauthorized search of Pursuit’s computer files to obtain litigation advantage constitutes, in the Court’s view, a “breach of the orderly disclosure scheme set forth in CPLR article 31” (*id.* at 570).

*Harleysville Ins. Co. v Holding Funeral Home, Inc.*, 2017 WL 1041600 [WD Va Feb. 9, 2017] [Magistrate Judge opinion], *objections sustained in part and overruled in part*, 2017 WL 4368617 [WD Va Oct. 2, 2017]) presented a somewhat similar set of facts, but with important differences. That case involved coverage litigation between an insured funeral home and its insurer (Harleysville). An employee for Harleysville put the entire case file, including privileged materials, on a file-sharing site (Box.com) which had no password protection, and then emailed a link to the site to Harleysville’s outside investigator. The funeral home issued a subpoena to the investigator, and the investigator’s production included the e-mail containing the link to

Box.com. The funeral home's counsel accessed the case file and downloaded the material, and then disseminated the Claims File to their clients and to law enforcement officials. Harleysville only found out about the disclosure when the funeral home later produced the case file back to Harleysville during discovery. Harleysville sought sanctions and to disqualify the funeral home's counsel.

The federal magistrate judge found that Harleysville waived attorney-client privilege and work product protection by placing the claim file on Box.com without password protection, and that disqualification of counsel was not warranted (*Harleysville*, 2017 WL 1041600, at \*5). Nevertheless, the magistrate judge held that the funeral home's counsel should have contacted Harleysville's counsel and revealed that it had access to this information, or alternatively should have asked the court to decide the issue of privilege waiver before making any use of or disseminating the information (*id.* at \*8). As a sanction, the magistrate judge awarded Harleysville its fees and costs incurred in pursuing the motion.

On review, the district court found that Harleysville's applicable privileges had *not* been waived. The court, like the magistrate judge, took a dim view of the funeral home's counsel's handling of the claims file: "Insureds' counsel violated [Federal] Rule 45(e)(2)(B) when they refused to return, sequester, or destroy the privileged material upon Harleysville's counsel's request. In addition, and perhaps more importantly, they failed to adhere to the ethical standards espoused by the Virginia State Bar. Attorneys must strive to avoid both impropriety as well as the mere appearance of impropriety in their conduct, and they must uphold the integrity of the profession. By attempting to conceal their possession of the Claims File and usurping the role of the court by making a unilateral determination on the issue of waiver, Insureds' counsel fell far short of their responsibility" (*id.* at \*14). The court imposed an evidentiary sanction, prohibiting



the funeral home from using any Harleystville privileged material, or information derived from such material, to seek additional information during discovery or to use such information in the litigation or any other related civil litigation. The court declined to disqualify counsel from the case.

Although the facts of *Harleystville* differ from the case here, the decisions in that case support the conclusion that Defendants' counsel should have acted differently when confronted with the obviously unintended "disclosure" of Pursuit's confidential information. The Court concludes that upon discovering that the hyperlink in the emails produced by Parzygnat allowed KrunchCash to access Pursuit's live corporate file directory, counsel should have realized that remotely rummaging through Pursuit's linked computer files was beyond the scope of legitimate litigation discovery (even assuming counsel voluntarily chose not to review the "Legal" files contained in the directory). The subsequent attempt to weaponize the information obtained exacerbates the matter.

Accordingly, Defendants (counsel and client) are ordered to reimburse Pursuit \$155,977, which represents Pursuit's reasonable attorneys' fees and costs in bringing this. However, the Court does not find that KrunchCash should be responsible for the \$9,860 in fees incurred by Pursuit to notify Pursuit's investors of a data breach. Such notifications would have likely been necessary even if KrunchCash had only spent 5 minutes in the DropBox before realizing that the DropBox was live. Since KrunchCash did not initially obtain access to the DropBox through improper means, this sanction is not warranted.

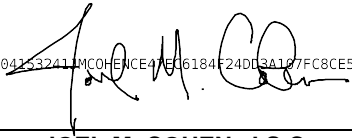
Accordingly, it is

**ORDERED** that Pursuit's Motion is **GRANTED** to the extent that the Court grants a protective order over all documents contained in Pursuit's DropBox that were not subsequently

produced by Pursuit in discovery. All such documents in the possession of KrunchCash or any of its employees, agents, or attorneys must be returned to Pursuit within five days of the date of this order. Any copies, descriptions, or summaries of such documents, whether attorney work product or otherwise, shall be destroyed immediately; and it is further

**ORDERED** that Defendants shall reimburse Pursuit in the amount of \$155,977, which represents Pursuit’s reasonable attorneys’ fees and costs in bringing this motion; Pursuit’s request for \$9,860 in notification fees is denied.

This constitutes the Decision and Order of the Court.

202310041532411MCOHEN47E6184F24D03A197FC8CE58EE3C0  
  
\_\_\_\_\_  
**JOEL M. COHEN, J.S.C.**

10/4/2023  
DATE

CHECK ONE:

CASE DISPOSED  
GRANTED  DENIED  
SETTLE ORDER  
INCLUDES TRANSFER/REASSIGN

NON-FINAL DISPOSITION  
GRANTED IN PART  OTHER  
SUBMIT ORDER  
FIDUCIARY APPOINTMENT  REFERENCE

APPLICATION:

CHECK IF APPROPRIATE: