

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF MISSISSIPPI
NORTHERN DIVISION**

**TLS MANAGEMENT & MARKETING
SERVICES, LLC**

PLAINTIFF

V.

CAUSE NO. 3:14-CV-00881-CWR-LRA

**MARDIS FINANCIAL SERVICES, INC.,
ET AL.**

DEFENDANTS

ORDER

A court does justice by finding truth. That search requires evidence. Intentionally destroying evidence, then, is more than a devious litigation strategy. It is a lethal attack on a court's purpose, and must be responded to in kind.¹

Federal Rule of Civil Procedure 37(e)(2) provides tools to do so.² Those tools address intentional destruction of “electronically stored information” – that is, data. People must preserve data they know (or should know) “may be relevant” to a lawsuit.³ The Rule says that, if such data is lost in bad faith, a court can enter a default judgment against the wrongdoer.⁴

¹ See *Stewart v. Belhaven Univ.*, No. 3:16-CV-744-CWR-LRA, 2017 WL 3995989, at * 4, n. 5 (S.D. Miss. Sept. 8, 2017).

² Similar tools are available through a court's inherent power to regulate the litigation process. But that power is used only when evidence destruction “occurs before a case is filed or if, for another reason, there is no statute or rule that adequately addresses the conduct.” *Rimkus Consulting Grp., Inc. v. Cammarata*, 688 F. Supp. 2d 598, 611 (S.D. Tex. 2010). The Rule adequately and justly addresses Defendants' conduct, and does so in the same way this Court's inherent power would. See *Barnett v. Deere & Co.*, 2:15-cv-2-KS-MTP, 2016 WL 4544052, at *2 (S.D. Miss. Aug. 31, 2016). The Court also has other potent tools in its arsenal, including one that ignites the criminal process and could lead to life altering consequences for a wrongdoer. See, e.g., *Devine v. Wal-Mart Stores, Inc.*, 52 F.Supp.2d 741, 746, n. 7 (S.D. Miss. 1999) (Court referring matter to the United States Attorney to determine if plaintiff who perjured themselves should be criminally prosecuted); *Wallace v. Ford Motor Co.*, No. 3:11-CV-567-CWR-FKB, 2013 WL 3288435, at *5 n.1 (S.D. Miss. June 28, 2013)(explaining that spoliation of evidence may subject party to criminal penalties and civil sanctions).

³ *Guzman v. Jones*, 804 F.3d 707, 713 (5th Cir. 2015) (describing the common law duty to protect lawsuit-relevant information). The Rule is “based on [this] common law duty” to preserve potential evidence. See Advisory Committee Notes to Fed. R. Civ. P. 37(e); *infra* at n. 6.

⁴ Fed. R. Civ. P. 37(e)(2)(C); see also *Guzman*, 804 F.3d at 713 (spoliation sanctions are “only available upon a showing of bad faith or bad conduct”).

TLS Management & Marketing Services says such wrongdoers include Todd Mardis and two businesses he runs, Capital Preservation Services and Mardis Financial Services. To agree, this Court must satisfy the five questions asked by the Rule.⁵

1. Was There Data Defendants Should Have Preserved?⁶

Yes.

This lawsuit alleges that – as former TLS contractors – Defendants profited by using stolen data about TLS’s tax business, products, and customers. To prove its claims (which are breach of contract, tortious business interference, unfair competition, violations of Mississippi trade secrets law, and violations of federal false advertising law), TLS needed data about Defendants’ business strategies, clients, and products.⁷ Defendants had to begin preserving that data the moment they were notified of TLS’s claims in 2014.⁸

Doing so meant protecting the containers where that data was “likely” stored.⁹ These containers included electronic documents and the places those documents were stored, such as computers, hard drives, and user profiles. Destroying those containers means losing the data they store.¹⁰ To preserve business data, then, Defendants could not destroy those containers.¹¹

⁵ The current version of the Rule applies here. See Supreme Court Apr. 29, 2015 Order, available at [https://www.supremecourt.gov/orders/courtorders/frcv15\(update\)_1823.pdf](https://www.supremecourt.gov/orders/courtorders/frcv15(update)_1823.pdf) (current version of the Rule applies to all civil proceedings pending on Dec. 1, 2015 “insofar as just and practicable”).

⁶ The Rule only applies to data that “should have been preserved in the anticipation or conduct of litigation.” Fed. R. Civ. P. 37(e).

⁷ The contract claim requires proof that Defendants used TLS’s business information. See *TLS Mgmt. & Mktg. Servs. LLC v. Mardis Fin. Servs. et. al.*, 3:14-CV-00881-CWR-LRA (S.D. Miss. Nov. 30, 2016) (discussing nature of relevant contracts). The trade secrets claim requires proof that certain business information was “[d]isclos[ed] or use[d].” Miss. Code Ann. § 75-26-3. The false advertising claim requires proof that a person used “false or misleading” commercial information. 15 U.S.C.A. § 1125(1). The unfair competition claim requires similar proof, see *Git-R-Done Prods., Inc. v. Giterdone C Store, LLC*, 226 F. Supp. 3d 684, 691 (S.D. Miss. 2016), as does the tortious business interference claim, see *Unified Brands, Inc. v. Teders*, 868 F. Supp. 2d 572, 578 (S.D. Miss. 2012).

⁸ They were notified on November 17, 2014, the day on which they were served with the Complaint.

⁹ *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216-18 (S.D.N.Y. 2003).

¹⁰ *Id.*; see also Declaration of Sean McDermott at 5, Docket No. 162-4 (deleting a user profile means losing “all user created files . . . located in the user profile folder hierarchy”); Deposition of Andy Mazingo at 53 (expert stating “correct” when asked if the “information[] in [a] user profile . . . would be forever lost if you deleted it”).

¹¹ Courts using their inherent power to weigh spoliation sanctions limit the scope of the duty to protect to documents that contain “unique” data. See, e.g., *Zubulake*, 220 F.R.D. at 216. The wise goal of this limit is to prevent parties

2. Did Defendants Lose That Data By Not Preserving It?¹²

Yes.

Defendants destroyed numerous containers that likely contained business data:

- In early 2017, Todd Mardis deleted hundreds of business documents on his computer.¹³
- In late 2016, Capital Preservation Services financial advisor David Byrd had his corporate computer thrown away after it “crashed.”¹⁴
- In August 2016, CPS financial director Kim Mardis deleted the user profile on her corporate computer.¹⁵
- In September 2016, CPS tax planning director Donna Carter deleted the user profile on her corporate computer.¹⁶ Later that year, Carter also deleted dozens of business documents from that same computer.¹⁷

from being punished for destroying duplicated documents. *Id.* The Rule rejects this limit, but achieves the same wise goal through its “cannot be restored or replaced” language. See *infra* at 4-6.

¹² The Rule applies only to data that was “lost because a party failed to take reasonable steps to preserve it.” Fed. R. Civ. P. 37(e).

¹³ See Logs of Files Deleted From Todd Mardis’s Computer, Exs. 6-18 at Docket No. 129. Todd Mardis deleted tens of thousands of files during this period, but the vast majority of those were system-created. See Expert Report of Sean McDermott at 8-11, Docket No. 129-1. Such files do not “likely” contain business data; therefore, Defendants did not need to protect them. See Zubulake, 220 F.R.D. at 217-18; Deposition of Michael Lenoir at 11-12, Docket No. 145-1 (explaining difference between user- and system-created files). Defendants appear to concede that Mardis deleted as many as 900 user-created documents. See Defendants’ Memorandum In Support of Their Response to Plaintiff’s Motion for Default Judgment, Docket No. 146. at 7, n. 8.

¹⁴ See Excerpts of David Byrd Deposition, Docket No. 129-52; Undated Email from Lawyer for Defendants, Docket No. 162-1; McDermott Report at 16. Defendants claim Byrd’s son threw away the computer after it crashed. This is irrelevant. Byrd was responsible for preserving the computer, and should have prevented his son from destroying it.

¹⁵ McDermott Report at 12-14.

¹⁶ *Id.* at 14-16.

¹⁷ *Id.*; Logs of Files Deleted From Donna Carter’s Computer, Docket No. 129-39.

There is no doubt this destruction happened, and that Defendants caused it.¹⁸ Todd Mardis, Kim Mardis, and Donna Carter all swore under oath that this destruction did not happen, and that they did not cause it.¹⁹ They lied.

3. Was The Destroyed Data Permanently Lost?²⁰

Yes.

Destroyed data is permanently lost unless it “can be found elsewhere.”²¹ Finding destroyed data can be simple, if a company systematically used back up tools.²² To prove they did so, Defendants must show “clear and convincing evidence that all information” – not some or most information – was likely backed up.²³

Defendants say they had a routine of backing up information using two tools: Dropbox and Microsoft Outlook.²⁴ Dropbox, which backs up documents in select parts of a user profile,²⁵ was used on many of Defendants’ computers.²⁶ The same is true of Microsoft Outlook,²⁷ which backs up all documents attached to emails received or sent on a computer.²⁸ But these facts only

¹⁸ No one but the owner of each relevant computer was responsible for the data destruction. See generally Deposition of Luke Lundemo, Docket No. 145-2; Lenoir Deposition, Docket No. 145-1 (testimony from Defendants’ computer technicians).

¹⁹ These denials came in April 2017, well after the destruction had occurred. See Todd Mardis Deposition Excerpts, Docket No. 129-49 (“I didn’t preserve or destroy documents”); Kim Mardis Deposition Excerpts, Docket No. 129-50 (denying awareness of “any reason” why business relevant documents would “no longer be available” for discovery); Donna Carter Deposition Excerpts, Docket No. 129-51 (same denial).

²⁰ The Rule applies only to data that “cannot be restored or replaced through additional discovery.” Fed. R. Civ. P. 37(e).

²¹ Advisory Committee Notes to Fed. R. Civ. P. 37(e).

²² See *TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo*, Civ. No. 15-21-21 (BJM), 2017 WL 1155743, at *2 (D.P.R. Mar. 27, 2017).

²³ *Id.* (emphasis added).

²⁴ Expert Report of Andy Mzingo at 14, Docket No. 145-4. Carbonite backup software was also used on a single corporate computer; however, there is no evidence that Carbonite backed up any lost data. See Lundemo Deposition at 10 (explaining Carbonite and its use by Defendants). Defendants also may have used a file backup system called ActionStep, but the record contains little discussion of this system. See, e.g., Lenoir Deposition at 8.

²⁵ Mzingo Report at 7 (explaining that Dropbox backs up data in a “folder” on a user profile “calle[d] ‘Dropbox’”).

²⁶ See generally *id.*

²⁷ *Id.*

²⁸ Lenoir Deposition at 16-17.

establish that Dropbox and Microsoft Outlook likely backed up some data. Defendants must show that all destroyed data was likely backed up.

To do so, Defendants commissioned an expert report.²⁹ It is wholly inadequate, leaving nearly every important question unanswered. How often did Defendants back up their data? The report does not say. What data, if any, on David Byrd's computer was backed up before it was thrown away? The report does not say – nor could it, given that its author never examined Byrd's computer.³⁰ What data, if any, on Donna Carter or Kim Mardis's user profiles was backed up before they were erased? The report does not say.³¹

The questions the report does answer do not help Defendants. How many of the hundreds of business documents deleted from Todd Mardis's computer were backed up? Just four, the report says.³² The report's author says he "saw" duplicates of the other documents,³³ but only documented a "random sampling" because doing otherwise "would have taken forever, and it would have cost \$50,000."³⁴ Defendants must live with the report they paid for.

Just as futile is Defendants' other attempt to show the destroyed data is recoverable. Defendants recently submitted the deposition of a technician who recovered "thousands" of

²⁹ See generally Mazingo Report.

³⁰ Mazingo Deposition, Docket No. 162-5, at 55 (expert stating he did not examine David Byrd's computer, nor was he aware it was destroyed).

³¹ The report briefly mentions the deletion of Kim Mardis's user profile, and says it was simply a "roll back" event. Mazingo Report at 12-13. However, the report never defines what a "roll back" event is, and its author says he "do[es not] know exactly the details of a roll back event" – except that "it's possible" a roll back event overwrites files on a computer. Mazingo Deposition at 53.

³² See Mazingo Report at 6-8, Appendix 3 (listing currently existing files with names similar to those of four documents deleted from Todd Mardis's computer).

³³ Mazingo Deposition at 21. However, when later asked if he "saw every single one" of the deleted documents, the expert said "that's not my testimony." Id.

³⁴ Id. at 20. The expert also testified that he "did not conduct any analysis to confirm that [those] other deleted user-created files . . . were recoverable." Id. at 21.

deleted files from Todd and Kim Mardis’s computers.³⁵ But Defendants submitted no analysis proving those files are relevant to this case. Tellingly, they never asked for one.³⁶

Defendants might have backed up a fraction of the destroyed data. But there is no clear and convincing evidence they backed up most of that data, which must be assumed permanently lost.

4. Was The Data Lost In Bad Faith?³⁷

Yes.

Bad faith is determined by the when and how of data loss. Bad faith data loss happens when, shortly after receiving a request to protect lawsuit-relevant data, a person destroys many documents that likely contained such data.³⁸ Bad faith data loss does not happen when, “well in advance” of such a request, “routine procedures” destroy lawsuit-relevant data.³⁹

Here, the when of data loss began when TLS filed this lawsuit in late 2014. For the next two years, despite many reasonable requests from TLS, Defendants refused to open their books.⁴⁰ In July 2016, TLS asked this Court to force those books open, noting that Defendants had “not produced a single document in response to any request for production.”⁴¹ As early as⁴²

³⁵ Lenoir Deposition at 13.

³⁶ Id. at 17 (“I don’t know if it recovered the files that he said were permanently deleted. I don’t know. I haven’t done any cross-comparison or list. . . . [I]f there was a File A and someone asked me to compare File B to File I and see if they were the same, I [would].”).

³⁷ Fed. R. Civ. P. 37(e)(2) and Advisory Committee Notes; see also Guzman, 804 F.3d at 713 (“Bad faith, in the context of spoliation, generally means destruction for the purpose of hiding adverse evidence.”).

³⁸ *OmniGen Research v. Yongqiang Wang*, 321 F.R.D. 367, 372 (D. Or. 2017), appeal dismissed sub nom. *OmniGen Research, LLC v. Yongqiang Wang*, No. 17-35519, 2017 WL 6507124 (9th Cir. Oct. 5, 2017); accord *Stewart*, 2017 WL 3995989, at *3 (explaining that party and her counsel’s breach of their duty to preserve evidence was a sanctionable discovery violation).

³⁹ *Vick v. Texas Employment Comm’n*, 514 F.2d 734, 737 (5th Cir. 1975).

⁴⁰ See, e.g., December 8, 2014 Motion to Dismiss or Stay Proceedings, Docket No. 10; March 16, 2015 Motion to Stay Disclosure Requirements, Docket No. 24; June 8, 2016 Motion for Protective Order, Docket No. 40; June 8, 2016 Motion to Quash Subpoenas, Docket No. 41; October 21, 2016 Motion for Protective Order, Docket No. 84; November 9, 2016 Motion for Protective Order, Docket No. 91; November 10, 2016 Motion to Quash Subpoena, Docket No. 91; November 21, 2016 Motion to Quash Subpoena & for Protective Order, Docket No. 99.

⁴¹ See TLS Memorandum in Support of Motion to Compel at 3, Docket No. 58.

⁴² The way Defendants destroyed data makes it hard to know when that destruction occurred. The fragments of data left on Defendants’ computers give ranges of dates that particular files could have been deleted. See McDermott

the following weeks, Kim Mardis and Donna Carter deleted their user profiles.⁴³ In November 2016, this Court held a hearing on TLS's request.⁴⁴ As early as the next day, Todd Mardis began deleting hundreds of business documents from his computer.⁴⁵ In December 2016, this Court granted TLS's request, and scheduled the examination of Defendants' computers.⁴⁶ In the weeks before that examination, David Byrd's computer was thrown away.⁴⁷ In sum, the when of this case strongly suggests bad faith data loss.

The how of data loss confirms that suggestion. Many documents deleted from the computers of Todd Mardis and Donna Carter had names like Marketing Agreement, Marketing and Tax Plan, Operating Agreement, and Engagement Agreement.⁴⁸ Deleting such files, erasing two user profiles, and throwing away a corporate computer – all in the midst of a business-related lawsuit – is convincing proof of bad faith.

There's more. Defendants used a cleanup tool called CCleaner on their corporate computers.⁴⁹ Permanently erasing data using CCleaner in the middle of a lawsuit is grounds for severe sanctions.⁵⁰ CCleaner does not automatically erase data; to do so, a user must take a host of deliberate steps.⁵¹ One step is clicking "OK" when asked, "This process will permanently

Report at 9-16. The "as early as" and similar language in this paragraph reflect those ranges, rather than the specific dates TLS misleadingly chose to use in its filings. See, e.g., TLS Memorandum at 12-17, Docket No. 130.

⁴³ *Supra* at nn. 15-16.

⁴⁴ November 30, 2016 Minute Entry.

⁴⁵ *Supra* at n. 13.

⁴⁶ *TLS Mgmt. & Mktg. Servs. LLC v. Mardis Fin. Servs. et. al.*, 3:14-CV-00881-CWR-LRA (S.D. Miss. Dec. 6, 2016).

⁴⁷ *Supra* at n. 14.

⁴⁸ *Supra* at nn. 13, 17.

⁴⁹ See generally McDermott Report.

⁵⁰ See *In re Abell*, No. 13-13847-TJC, 2016 WL 1556024, at *22-25; *Lexpath Techs. Holdings, Inc. v. Welch*, 13-cv-5379-PGS-LHG, 2016 WL 4544344, at *4 (D.N.J. Aug. 30, 2016); *Taylor v. Mitre Corp.*, 1:11-cv-01247 (LO/IDD), 2012 WL 5473715, at *9 (E.D. Va. Sept. 10, 2012).

⁵¹ *Id.* at 4; McDermott Affidavit at 6-16; see also *In re Abell*, 2016 WL 1556024, at *13-16 (Bankr. D. Md. Apr. 14, 2016) (detailed description of CCleaner's destructive capabilities). TLS has regularly framed CCleaner as devilish "anti-forensic software," whose installation necessarily proves bad faith. See, e.g., TLS's Reply in Support of Motion for Default at 1-3, Docket No. 162. If that is true, this Court is in trouble, as it has CCleaner on its own computer. Of course, TLS's framing is incorrect. Many businesses use that tool for entirely reasonable purposes. See

delete files from your system. Are you sure you wish to proceed?”⁵² CCleaner erases all traces of deleted files (called “metadata”⁵³), leaving a unique pattern of symbols on a hard drive.⁵⁴

That pattern appears on Todd Mardis’s hard drive,⁵⁵ and probably appears on Kim Mardis and Donna Carter’s hard drives.⁵⁶ It is unclear when the patterns on Todd Mardis’s hard drive were created, as he erased his software installation records.⁵⁷ What is clear is that Kim Mardis installed and ran CCleaner on February 19, 2016⁵⁸ – days after TLS asked Defendants to save all lawsuit-related data.⁵⁹ In the weeks before TLS was scheduled to examine Defendants’ computers, Kim Mardis ran CCleaner seven times.⁶⁰

The evidence that Defendants acted in bad faith – unlike the evidence Defendants used to show that all the destroyed data had been backed up – is clear and convincing. Defendants permanently erased data using CCleaner in the face of an ongoing lawsuit. Combined with the other evidence of bad faith data destruction, this shows Defendants to be egregious wrongdoers.

generally *In re Abell*, No. 13-13847-TJC, 2016 WL 1556024; Lundemo Deposition at 11-12. Defendants’ particular use of CCleaner proves their bad faith, not their mere installation of the software.

⁵² McDermott Declaration at 21-26.

⁵³ See Mazingo Report at 6 (defining metadata).

⁵⁴ McDermott Declaration at 9-13; *In re Abell*, No. 13-13847-TJC, 2016 WL 1556024, at *15.

⁵⁵ McDermott Report at 9-11 (describing patterns on Todd Mardis’s hard drive); McDermott Affidavit at 10-17 (explaining that many of those patterns could only have been created using CCleaner).

⁵⁶ The patterns on these hard drives – unlike those on Todd Mardis’s – appear to have consisted of all zeroes. *Id.* at 11-15. It is possible, though unlikely, that such patterns reflect unused (rather than erased) hard drive space. See Mazingo Report at 10.

⁵⁷ McDermott Report at 11.

⁵⁸ *Id.* at 11-12.

⁵⁹ February 12, 2016 and February 15, 2016 Emails from TLS Attorney to Defendants’ Attorneys, Docket No. 129-35.

⁶⁰ Prefetch Report Regarding CCleaner on Kim Mardis’s Computer, Docket No. 129-27. The report shows that the cleanup tool was run at different times of the day, strongly suggesting that this was user-initiated cleanup events, rather than automatic cleanup.

5. Is Default Judgment Appropriate?⁶¹

Yes.

The Rule allows courts to punish data destroyers with default judgment, but only when that punishment fits the crime.⁶² The measure of that crime is not the harm to the opposing party, but is rather the severity of data destruction.⁶³ Thus, default judgment is appropriate only when “destruction of evidence was of the worst sort: intentional, thoroughgoing, and (unsuccessfully) concealed.”⁶⁴

Such destruction occurred in *OmniGen Research v. Yongqiang Wang*.⁶⁵ There, companies filed contract and tort claims against a former employee, alleging he stole their trade secrets.⁶⁶ “[E]xtensive evidence” proved that the employee had responded by having “intentionally deleted thousands of documents,” “intentionally deleted . . . relevant emails from multiple email accounts,” “intentionally destroyed metadata,” and “donated [a] computer to Goodwill.”⁶⁷ This destruction “deprived the Plaintiffs of evidence central to their case and undermined the Court’s

⁶¹ The Rule allows a court to “presume that the lost information was unfavorable to the party,” “instruct the jury that it may or must presume the information was unfavorable to the party,” or “dismiss the action or enter a default judgment.” Fed. R. Civ. P. 37(e)(2). However, the Advisory Committee Notes state that “[t]he remedy should fit the wrong.”

⁶² Default judgment is inappropriate when “lesser” punishments can fix the loss. Advisory Committee Notes to Fed. R. Civ. P. 37(e)(2); accord *Union Pump Co. v. Centrifugal Tech. Inc.*, 404 F. App’x 899, 906 (5th Cir. 2010) (“Spoliation is a serious offense and a party’s intentional destruction of relevant evidence threatens the sanctity and spirit of the judicial process. However, the imposition of sanctions under the court’s inherent power is powerful medicine that should be administered with great restraint.”).

⁶³ The Advisory Committee Notes state that the Rule “does not include a requirement that the court find prejudice to the party deprived of the information,” as the finding of intent includes an assumption that “the opposing party was prejudiced by the loss of information.” “This is logical because ‘once spoliation is shown, the burden of proof logically shifts to the guilty party to show that no prejudice resulted from the spoliation because that party is in a much better position to show what was destroyed and should not be able to benefit from its wrongdoing.’” *OminGen*, 321 F.R.D. at 372. Defendant’s argument that TLS must show prejudice is rejected.

⁶⁴ *Gutman v. Klein*, 03 CV 1570(BMC)(RML), 2008 WL 4682208, at *12 (E.D.N.Y. Oct. 15, 2008), report and recommendation adopted, 2008 WL 5084182 (E.D.N.Y. Dec. 2, 2008); see also *Harper Macleod Solicitors v. Keaty & Keaty*, 260 F.3d 389, 393 (5th Cir. 2001) (“Federal courts generally disfavor default judgments.”).

⁶⁵ *Supra* at n. 38.

⁶⁶ *Id.* at 370.

⁶⁷ *Id.* at 372-77.

ability to enter a judgment based on the evidence. For these reasons, default judgment and terminating sanctions for the spoliation of evidence [was] warranted.”⁶⁸

The logic of *Omnigen* appears in similar cases,⁶⁹ and it applies here. Defendants knew they had data relevant to this lawsuit, and spent years resisting its discovery⁷⁰. Resistance failing, they systematically destroyed places that data was stored. Defendants took extraordinary steps to disguise that destruction, including lying under oath and permanently erasing data. This is more than ordinary wrongdoing. It is unacceptable. It is an assault on this Court’s ability to find truth, to do justice. The sanctions imposed here have been earned.

TLS’s motion for default judgment against all Defendants is GRANTED. All other pending motions are DENIED.⁷¹ The Court will contact the parties to set a status conference to be held during the week of February 5th, 2018 to discuss the setting of the trial on damages.

SO ORDERED, this the 29th day of January, 2018.

s/ Carlton W. Reeves
UNITED STATES DISTRICT JUDGE

⁶⁸ Id. at 372.

⁶⁹ See, e.g., *Glob. Material Techs., Inc. v. Dazheng Metal Fibre Co.*, No. 12 CV 1851, 2016 WL 4765689, at *9-10 (N.D. Ill. Sept. 13, 2016) (entering default judgment on a trade secrets claim because defendants “disposed of [corporate] computers while the lawsuit was pending,” “eras[ed] email[s],” “lied” about the extent of their destruction, and “stubborn[ly] fail[ed] to comply with their [discovery] obligations”).

⁷⁰ To be clear, parties have a right to use the rules to their advantage. The rules can be used as both weapons and shields. Parties have a right to seek refuge from a court’s ruling by appealing that decision. But parties have no right to destroy evidence.

⁷¹ These motions are denied WITH PREJUDICE, with the exception of TLS’s motion for leave to amend at Docket No. 137, which is denied WITHOUT PREJUDICE. Given Defendants’ conduct and their confusing maze of business entities, “the need might arise to attempt to pierce the corporate veil and hold the parent corporation liable.” *Flores v. Bodden*, 488 F. App’x 770, 777 (5th Cir. 2012) (citation omitted); see also *Bridas S.A.P.I.C. v. Gov’t of Turkmenistan*, 345 F.3d 347, 359 (5th Cir. 2003). If necessary, TLS may still make that attempt.