EVAN FINKEL (SBN 100673)
evan.finkel@pillsburylaw.com
MICHAEL S. HORIKAWA (SBN 267014)
michael.horikawa@pillsburylaw.com
CHAZ M. HALES (SBN 324321)
chaz.hales@pillsburylaw.com
CHLOE STEPNEY (SBN 334013)
chloe.stepney@pillsburylaw.com
PILLSBURY WINTHROP SHAW PITTMAN LLP
725 South Figueroa Street, 36th Floor
Los Angeles, CA 90017p
Telephone: 213.488.7100
Facsimile: 213.629.1033

CALLIE A. BJURSTROM (SBN 137816)
callie.bjurstrom@pillsburylaw.com
MICHELLE A. HERRERA (SBN 209842)
michelle.herrera@pillsburylaw.com
PILLSBURY WINTHROP SHAW PITTMAN LLP
11682 El Camino Real, Suite 200
San Diego, CA 92130
Telephone: 858.509.4000
Facsimile: 619.819.4363

[Additional counsel listed on last page]

Attorneys for Plaintiff
MICROVENTION, INC.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MICROVENTION, INC., a Delaware corporation,

Plaintiff,

vs.

BALT USA, LLC, a Delaware Limited Liability Company; DAVID FERRERA; NGUYEN "JAKE" LE; YOSHITAKA KATAYAMA; STEPHANIE GONG; AND MICHELLE TRAN,

Defendants.

Case No. 8:20-cv-02400-JLS-KES

MICROVENTION, INC.'S REPLY BRIEF IN SUPPORT OF ITS MOTION FOR SANCTIONS AGAINST DEFENDANT BALT USA, LLC FOR EVIDENCE SPOLIATION

Date: May 5, 2023
Time: 10:30 a.m.
Courtroom: 8A

Pre-Trial Conf.: August 4, 2023
Trial: To be Set

Hon. Josephine L. Staton

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. REPLY ARGUMENT 2

A. Balt's False Representation Regarding Encryption Keys Caused the Destruction of Evidence on the Tran and Katayama Laptops ... 2

B. Balt's False Representation to Stroz is an Affirmative Act That Caused the Data Loss 4

C. Stroz Was Not Responsible for Managing Balt's Encryption Keys 7

D. Balt's Expert Is Wrong About What Triggers BitLocker Recovery 9

E. Balt's Efforts to Search for the Encryption Keys Were Abysmal . 11

F. The Evidence Balt Destroyed is the Data Residing on the Tran and Katayama Laptops, Not the Encryption Keys Within Them 14

G. The Court Has Inherent Power to Fashion Appropriate Sanctions for Evidence Spoliation 16

III. CONCLUSION 18

TABLE OF AUTHORITIES

Page(s)

Cases

America Unites for Kids v. Rousseau,
985 F.3d 1075 (9th Cir. 2021). (Op. Br. 12:19–25.) 16

Apple Inc. v. Samsung Elecs. Co.,
881 F. Supp. 2d 1132 (N.D. Cal. 2012) 4

Aramark Mgmt., LLC v. Borgquist,
2021 WL 864067 (C.D. Cal. Jan. 27, 2021) 15

Farella v. City of New York,
2007 WL 193867 (S.D.N.Y. Jan. 25, 2007) 14

In re Google Play Store Antitrust Litig.,
2023 WL 2673109 (N.D. Cal. Mar. 28, 2023) 6, 8

Hamilton v. Signature Flight Support Corp.,
2005 WL 3481423 (N.D. Cal. Dec. 20, 2005) 16

Nat'l Ass'n of Radiation Survivors v. Turnage,
115 F.R.D. 543 (N.D. Cal. 1987) 7

Phan v. Costco Wholesale Corp.,
2020 WL 5074349 (N.D. Cal. Aug. 24, 2020) 6

Scalia v. County of Kern,
2023 WL 2333542 (E.D. Cal. Mar. 2, 2023) 16, 17

In re Skanska USA Civ. Se. Inc.,
340 F.R.D. 180 (N.D. Fla. 2021) 4, 5

Youngevity Int'l v. Smith,
No. 3:16-CV-704-BTM-JLB, 2020 WL 7048687 (S.D. Cal. July 28, 2020) 4, 5, 6, 8

Rules and Regulations

Federal Rules of Civil Procedure,
Rule 37 ..... 8, 15, 16

I. INTRODUCTION

In its opposition, Balt deliberately confuses the issues before the Court instead of addressing them head on, and plays the blame game instead of facing the harsh reality that Balt's conduct alone caused the destruction of evidence residing on the Tran and Katayama laptops. In fact, Balt places all of the blame on Stroz, whom ***Balt*** selected from a list of forensic analysts provided by MVI. In doing so, Balt completely ignores the undisputed fact that Stroz took the actions it did ***based on Balt's affirmative representation*** that Balt had all necessary encryption keys for its laptops and could and would provide them to Stroz. That statement was false, and Balt made it without any legitimate basis for believing it to be true. Stroz employed industry best practices based on the specific representation made by Balt, and shoulders no responsibility for the data loss.

Balt pays short shrift to the misrepresentation it made to Stroz, and only offers a *non sequitur* in response, *i.e.*, Balt's representation was not untrue because Balt believed encryption keys were not needed when it made the laptops available to Stroz. That makes no sense. Balt conducted ***no*** investigation and made ***no*** inquiries into whether or not it had the encryption keys before affirmatively misleading Stroz into believing that it did. Had it conducted an investigation before making its representation it would have discovered that it did not have the keys, and presumably would have made Stroz aware of that critical fact. Moreover, knowing that it did not have the encryption keys, Balt could have and should have retrieved them from the laptops when it booted them (albeit without a legitimate basis) using the process described by Balt's forensic expert.

Balt also deliberately misconstrues the evidence loss at issue in this motion. A constant refrain throughout Balt's opposition is that it could not have lost the encryption keys because it never had them. But the encryption keys are not the evidence that was destroyed. The data on the Tran and Katayama is the evidence that was destroyed, all at the hands of Balt. Balt did not lose the encryption keys in any event. They are in the laptops, but Balt inexplicably failed to store them anywhere else.

An adverse inference instruction is warranted. Balt's deliberate actions caused the data loss, period. The resulting prejudice to MVI from Balt's actions is monumental.

II. REPLY ARGUMENT

A. Balt's False Representation Regarding Encryption Keys Caused the Destruction of Evidence on the Tran and Katayama Laptops

The critical fact in MVI's motion – one that Balt does not dispute – is that before Stroz began the imaging process for the Tran and Katayama laptops, Balt ***affirmatively represented to Stroz*** that Balt had ***all of the encryption keys Stroz might need*** for the laptops when, in fact, Balt did not. Balt's misrepresentation is the sole cause of the complete and irretrievable loss of all the evidence residing on the Tran and Katayama laptops.

The first step in the preparation process for creating a forensic image of a laptop hard drive is to ensure that encryption keys are available for the laptop because different forensic imaging methods are used depending upon whether the encryption keys are available. (Declaration of Michael Bandemer ("Bandemer"), ¶¶7–9.) To that end, Sergio Kopelev, the principal for Stroz, stated in multiple planning calls with both MVI and Balt that encryption keys were needed for the laptops. (Declaration of Chaz Hales ("Hales"), ¶¶2–3.) In a final confirmation email four days before the scheduled imaging, Mr. Kopelev asked Balt to "[l]et us know if you have the information regarding any encryption keys and/or user name / passwords." (Dkt. 385-6, p. 27.) Balt confirmed via email that same day that it had the encryption keys, and promised it would "also have a representative from Balt's IT department on hand ***who will be able to unlock any encryption*** and provide user names and passwords." (*Id.* (emphasis added).)

Based on Balt's affirmative representation that it had the encryption keys for the laptops to be imaged, Stroz used industry standard techniques—techniques endorsed by Balt's own forensics expert, Ashraf Massoud—to image all of the laptops Balt provided

for imaging, including the Tran and Katayama laptops.[1] (Bandemer, ¶¶6–8; Dkt. 386-3, p. 34.) Mr. Kopelev explained that Stroz "changed a setting in the computer firmware to allow booting from an external device," which is a standard step taken "when the necessary decryption information (PIN, recovery key, etc.) is known." (Dkt. 386-3, p. 34.) Only ***after*** Stroz took that step, however, did Balt IT inform Stroz "that they did not have decryption information for the [Tran and Katayama] systems." Mr. Kopelev responded "***there was no indication that this was even a concern prior***" to that time. (*Id.* (emphasis added).) Stroz proceeded to image the Tran and Katayama laptops using an alternate method "with the understanding that while Balt IT didn't have the particular keys on hand, that they could be located at a later date for decryption." (*Id.*)

Stroz successfully analyzed all of the other encrypted laptop images it made that day, as well as the other encrypted laptop images Balt provided to Stroz. (Dkt. 385-6, pp. 22–24.) This is because Balt located the encryption keys for those devices, as it had represented it would to Stroz. (*Id.*) Only the Tran and Katayama laptops remained locked—not because Stroz used inappropriate methods as Balt now speculates, but because Balt did not have those encryption keys. Had Stroz known that the encryption keys were missing, it could have used other methods to image the laptops, including booting the laptops to create a live (rather than forensic) image and/or attempting to retrieve the encryption keys from the laptop first. (Bandemer, ¶¶4, 9.) For Stroz, Balt's affirmative representation that "the necessary decryption information [was] known" indicated one path of a decision tree for imaging rather than another.

The complete loss of data on the Tran and Katayama's laptops is Balt's failing, not Stroz's.

[1] Stroz imaged seven laptops provided by Balt and took receipt of five additional laptop images that Balt had previously created. (Dkt. 386-3, pp. 23–24, 28.)

B. Balt's False Representation to Stroz is an Affirmative Act That Caused the Data Loss

When Balt represented to Stroz on April 15, 2022, that it had the encryption keys for all laptops Balt provided to Stroz for imaging, Balt had taken ***no steps to verify whether that representation was true.*** (Hales, ¶7, Ex. 2, 104:19–23.) Balt did not even look for the encryption keys before making this sweeping affirmative statement, and instead blindly assumed they would magically appear when needed. Had Balt properly investigated the matter, it would have easily determined that it did not, in fact, have the encryption keys for the Tran and Katayama laptops and could have alerted Stroz who would have responded accordingly. (Dkt. 385-6, p. 19.) Balt acted with conscious disregard of its discovery obligations when it made this unequivocal representation to Stroz about a critical issue without conducting any due diligence whatsoever regarding the accuracy of the representation. *See Apple Inc. v. Samsung Elecs. Co.*, 881 F. Supp. 2d 1132, 1146–47 (N.D. Cal. 2012) (defendant's conscious disregard of its obligations to preserve evidence was "more than sufficient to show willfulness" necessary for adverse inference instruction); *Youngevity Int'l v. Smith*, No. 3:16-CV-704-BTM-JLB, 2020 WL 7048687, at *2–3 (S.D. Cal. July 28, 2020) (defendants would not be excused from taking affirmative action to prevent destruction even if unaware deletion functions were in place on devices).

Balt tries to distinguish the facts of the present case from *In re Skanska USA Civ. Se. Inc.*, 340 F.R.D. 180 (N.D. Fla. 2021), cited by MVI in its moving papers, by arguing that it "engaged in no affirmative act causing evidence to be lost." (Balt Opposition Brief, Dkt. 409 ("Op. Br."), 10:5–6.) That is simply not true. Balt made an affirmative representation to Stroz, in writing, that it had the encryption keys for the laptops to be imaged. This affirmative representation led directly to the imaging method selected by Stroz. To the extent the chosen imaging method may have caused the locking of the laptops and loss of data, Stroz selected its chosen method in reliance on Balt's affirmative yet demonstrably false representation. (Dkt. 386-3, p. 34.) Balt's failure to

do anything to preserve the data on its encrypted laptops, and specifically its failure at any point to secure the encryption keys needed to provide access to the laptops, constitutes an affirmative act.

Balt claims it "has provided a credible explanation for the locking of the laptops[,]" and that Balt should therefore be off the hook for its destruction of key evidence in this case.. (Op. Br., 10:11–12.) But Balt's explanation is misplaced. *Skanska* requires a credible explanation of the affirmative act—in this case Balt's affirmative false representation to Stroz that it possessed the encryption keys. Balt provides no explanation at all, much less a credible one, for the misrepresentation it made to Stroz.

Further, "[t]he existence of reasonable explanations for why deletions occurred does not suggest that reasonable steps were taken to prevent deletions." *Youngevity*, 2020 WL 7048687, at *2. This important distinction is lost on Balt. Balt's purported "innocent" belief that there was no encryption on the laptops because Balt IT personnel had successfully logged into the laptops the day before they were imaged does not stand up to scrutiny. As a preliminary matter, Balt should not have booted the laptops; booting the laptops is itself an act of evidence destruction. (Bandemer, ¶¶4–5.) Booting a laptop alters the evidence stored on that laptop and is to be avoided in creating a forensic image so as to not "risk[] modification or deletion of data present on the [laptop]." (Hales (Sergio email).) (*Id.*, Dkt. 386-3, p. 34.)

Moreover, logging into a laptop does not reveal whether BitLocker encryption, which is part of the Windows operating system, is enabled or not. (Bandemer, ¶16.) Balt's own expert explains that logging into an encrypted laptop is the first step in the "easy" process of exporting the encryption keys from encrypted laptops. (Declaration of Ashraf Massoud, Dkt. 411 ("Massoud"), ¶8.) And, Balt's IT Director for Global Operations testified that he (1) knew many of Balt's laptops were encrypted, (2) had debriefed a departing IT employee only a month prior to the imaging on topics including how Balt sets up BitLocker encryption on its laptops and stores encryption keys, and

(3) was leading efforts to improve the way Balt stores laptop encryption keys. (Ex. 1 to Hales, 61:17–62:10, 86:10–88:14, 63:11–66:6.) It is not reasonable to conclude from simply booting a laptop that it is not encrypted, and the statements by Kheng Ang in his declaration are inconsistent with his deposition testimony given in this case. (Bandemer, ¶16.)

In addition, Balt arrived at its erroneous conclusion after booting the laptops on April 18—three days after it made its representation to Stroz that it had the encryption keys yet before the imaging process began. (Dkt. 385-6, pp. 2, 23, 27.) At no point did Balt provide any update to Stroz about what it had done with the laptops or the erroneous conclusion it had reached regarding the encryption keys. (Hales, ¶4.) Had Balt promptly shared this information with Stroz, standard practices dictate that alternative means for imaging the laptops would have been undertaken. (Bandemer, ¶¶7–9.) Balt's decision to keep this important information to itself on the eve of imaging the laptops was deliberately reckless, at the very minimum. *See Phan v. Costco Wholesale Corp.*, 2020 WL 5074349, at *3 (N.D. Cal. Aug. 24, 2020) (finding the "absence of evidence of a proper process for preserving [] important evidence indicates, at a minimum, that defendant was careless"); *In re Google Play Store Antitrust Litig.*, 2023 WL 2673109, at *9 (N.D. Cal. Mar. 28, 2023) (concluding defendant's poor management of efforts to preserve relevant chat messages "fell strikingly short" of its discovery obligations); *Youngevity*, 2020 WL 7048687, at *2 (finding defendants' "ignorance" of automatic message deletion and failure to back up devices was "no defense because their preservation obligation necessarily entailed learning of these systems to prevent destruction"). None of Balt's actions, and deliberate failure to act, are innocent or inconsequential, and all of it led directly to the loss of the critical evidence on these key laptops.

Of significance, having booted the laptops the day before the imaging was to take place, Balt failed to do any of the things that would have preserved the encryption keys. (Bandemer, ¶¶5, 9.) Balt failed to follow its expert's "easy" instructions to export the

encryption keys from the BitLocker control panel. Balt also failed to use the control panel to "suspend" BitLocker operation, which is a step recommended by Microsoft prior to engaging in planned activities that could trigger a BitLocker recovery mode. (Bandemer, ¶14.) Had Balt undertaken either of these measures, the evidence would not have been lost.

C. Stroz Was Not Responsible for Managing Balt's Encryption Keys

Balt blatantly attempts to shift the blame for its data loss to Stroz and tries to distance itself from Stroz by characterizing it as the firm that "MVI proposed." (Op. Br., 2:27–3:1.) The record is clear that MVI proposed three acceptable vendors, and ***Balt*** selected Stroz from that list.[2] (Exs. 1–2 to Declaration of Paul Stewart, Dkt. 410-1, pp. 2, 6.) Regardless, Balt completely ignores the affirmative representation it made to Stroz that it had the encryption keys for all laptops Stroz was tasked with imaging, and fails to meaningfully address it in its Opposition Brief.

Instead, Balt incredulously argues that Stroz—not Balt—was responsible for managing Balt's encryption keys. According to Balt's forensics expert, the encryption keys are stored in the laptops themselves and can be easily retrieved by "logging into the computer [with local admin rights], opening the Control Panel, and clicking on the BitLocker icon." (Massoud, ¶¶ 5, 8.) He opines that ***Stroz*** "should have logged onto the [laptops] using the administrative user name and password provided by Balt" and "easily retrieved [the encryption keys] from the Windows Control Panel." (Massoud, ¶ 15.) In fact, after Balt later informed Stroz that it could not locate any other copies of the encryption keys, it sent the laptops to Stroz's lab in Boston, and Stroz did attempt to log into the laptop with the admin credentials. (Dkt. 385-6, p. 5.) Only then, on May 2, 2022, did Stroz and the parties learn that the laptops were completely inaccessible

[2] Balt liberally misstates facts in its brief. For example, MVI did not ask previously ask Judge Scott to find Balt "guilty of spoliation." (Op. Br., 3:6.) MVI mentioned spoliation within the context of its motion to compel Balt to provide information regarding its litigation hold memorandum (Dkt. 229-1), which Judge Scott granted. Judge Scott made no finding on spoliation. (*See* Ex. 4 to Stewart, 13:10–14:4.)

unless Balt could find a copy of the encryption key stored some other place.

This begs the obvious question: If Stroz could have retrieved the encryption keys so easily, why didn't Balt do so ***before*** it provided the laptops to Stroz? These are ***Balt laptops***, issued to ***Balt employees***, managed by the Balt ***IT department***, and for which ***Balt*** is under an obligation to preserve the evidence (i.e., documents and files) stored on the laptops for use in this litigation. *Nat'l Ass'n of Radiation Survivors v. Turnage*, 115 F.R.D. 543, 557–58 (N.D. Cal. 1987) ("The obligation to retain discoverable materials is an affirmative one."). Moreover, just three days after Balt told Stroz that it had all encryption keys and one day before Balt made the laptops available to Stroz for imaging, ***Balt booted the laptops*** and had every opportunity at that time to "simply" retrieve the encryption keys. That would have been the prudent and expected course of action by Balt to (1) ensure the integrity and accessibility of the laptops and (2) confirm that Balt's representation about having all encryption keys necessary to access the laptop contents was accurate. (Bandemer, ¶¶5, 9, 17.) Balt did neither and its attempt to pass off its own IT failures as Stroz's fault is an act of desperation.

Lastly, Balt's expert does not address the fact that Balt ***failed*** to store the encryption keys for its employee laptops in a safe location—somewhere other than on the laptops themselves—or secure the encryption keys when its duty to preserve evidence arose. (Bandemer, ¶15.) "As Rule 37 indicates, the duty to preserve relevant evidence is an unqualified obligation in all cases." *In re Google Play Store Antitrust Litig.*, 2023 WL 2673109, at *8 (N.D. Cal. Mar. 28, 2023). The record shows that Balt did not have a consistent or effective procedure in place to track and store laptop encryption keys before MVI filed this lawsuit. (Hales, ¶7, Ex. 1, 63:11–66:6.) However, Balt cannot now rely on its inadequate IT practices as an excuse for its failure to preserve evidence on its employee laptops. *See* Fed. R. Civ. P. 37, Advisory Committee Notes to the 2006 Amendment ("[A] party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue."); *Youngevity*, 2020 WL 7048687, at *2 (S.D. Cal. July 28,

2020) ("Although perfection is often impossible in preserving ESI within complex electronic systems because it may be 'lost as a result of the routine good faith operation' of the system, this does not excuse the party from preventing destruction within their control."). Balt's conduct destroyed evidence that was clearly within its control.

D. Balt's Expert Is Wrong About What Triggers BitLocker Recovery

Balt's attempt to shift blame to Stroz is built on a house of cards. Balt's expert explains that sometimes a forensic examiner must modify the computer's BIOS program "so that the computer starts up by accessing a drive attached to a USB port" rather than its internal hard drive, which allows the examiner to then boot from a USB device containing forensic software that is used to image the hard drive in an "off" state. (Massoud, ¶¶ 10–12; Bandemer, ¶11.) Mr. Massoud then incorrectly guarantees that "[a]ltering the BIOS/UEFI program instructions in this manner ***will not cause the computer to lock***." (Massoud, ¶ 12 (emphasis added).)

This is simply not true. In direct contrast, Microsoft's "BitLocker recovery guide" lists changing the BIOS in order to boot from "something other than the hard drive" among a list of 30 "specific events that ***will cause*** BitLocker to enter recovery mode when attempting to start the operating system drive." (Bandemer, ¶¶12–14, Ex. 1, p. 5.) In fact, Mr. Kopelev's description of the steps Stroz took ***match*** Mr. Massoud's recommended "safe" procedure exactly. Stroz "changed a setting in the computer firmware [BIOS/UEFI program instructions] to allow booting from external media [a drive attached to a USB port]." (*Compare Dkt. 386-3, p. 34, with Massoud, ¶12.*) Unlike Mr. Massoud, who incorrectly stated that such a procedure "will not" trigger the BitLocker recovery mode, Mr. Kopelev acknowledged that this process could, indeed, have triggered BitLocker and explained that the process is standard "***when the*** necessary ***decryption information . . . is known***." (Dkt. 386-3, p. 34 (emphasis added).)

Mr. Massoud compounds his error by blindly surmising that "***[b]ecause*** the laptops were locked by BitLocker," Stroz clearly "did something" that BitLocker interpreted as "tampering." (Massoud, ¶17.) Mr. Massoud further speculates that Stroz

"may have" turned off a feature called Secure Boot, and claims that if someone turns off Secure Boot, the computer "will require the BitLocker key." (Massoud, ¶¶13, 17.) Mr. Massoud then continues his proclivity to read minds by proffering, without any foundation whatsoever, that Stroz "apparently believe[d] incorrectly that [turning off Secure Boot] was necessary" before confidently declaring that "this step was not necessary" and fingering the disabling of Secure Boot as the "likely" reason the Tran and Katayama laptops were locked. (Massoud, ¶17.)

Mr. Massoud's speculative hypotheses are riddled with problems. First, as has been stated, there is no need to look for an alternate explanation. Mr. Massoud's own recommended method of imaging laptops that Stroz employed is on Microsoft's list of things that can trigger BitLocker. (Bandemer, ¶13, Ex. 1.) Second, the list is not short, and it is unclear why "disabling Secure Boot," which ***does not appear on the list***, catches Mr. Massoud's attention. (*Id.*) Third, there has been no evidence or testimony proffered at any point indicating that Secure Boot was enabled on any Balt laptop such that Stroz could have disabled it. Fourth, there is likewise no evidence that Stroz disabled the Secure Boot setting or modified it in any way. Mr. Kopelev's explanation does not mention Secure Boot and, instead, straightforwardly explains that the BIOS was modified to allow booting from an external [USB] device. (Dkt. 386-3, p. 34; Hales, ¶5.)

Nevertheless, Balt attempts to capitalize on Mr. Massoud's flawed conclusion by converting Mr. Massoud's qualified and speculative opinions to unqualified and absolute conclusions. (Op. Br., 2:3 ("Stroz Friedberg took an extra and unnecessary step"); 4:21–23 ("due to a mistake [Stroz] made in the process"); 5:1 (Stroz "took an extra and unnecessary step relating to the BIOS"); 5:23 ("If Stroz Friedberg had not turned off the 'Secure Boot' setting"); 8:16–17 (Stroz "apparently chose to turn off the 'Secure Boot' setting in the BIOS program"); 8:19–21 (Stroz "unnecessarily triggered the BitLocker encryption software by apparently turning off the 'Secure Boot' setting"); 10:8–10 (Stroz "chose to take the unnecessary step of turning off the laptop's 'Secure

Boot' setting in the BIOS program"); 11:5–6 (Stroz could have accessed the encryption keys "if [it] had followed best practices"); 13:3–5 (Balt "had no way of knowing[] that Stroz Friedberg would turn off the 'Secure Boot' setting"); 13:19–20 ("if [Stroz] did not make the mistake of turning off [Secure Boot]"); 14: 18–19 ("Stroz Friedberg made a mistake").

Lost in the din is an admission that Balt cannot escape: "Balt is not privy to the specific technique Stroz Friedberg used." (Op. Br., 4:25–26.) Balt does not know because it did not ask Stroz for ***any*** information about the steps Stroz took when imaging the laptops after receiving Stroz's explanation on May 13, 2022. (Hales, ¶5.) MVI is unaware of any communications between Balt and Stroz discussing Secure Boot or any other details of how Stroz imaged the laptops aside from Mr. Kopelev's email. (*Id.*) Anything further that Balt attributes to Stroz is unfounded, based only on self-serving speculation, and premised on an incorrect understanding of how BitLocker works. Balt's "could have, should have, would have" scenarios are part of Balt's overarching smoke and mirrors game designed to obfuscate the issues and distract the Court's attention away from Balt's egregious and irremediable errors and should be given no weight.

E. Balt's Efforts to Search for the Encryption Keys Were Abysmal

Balt paints itself not only as Stroz's innocent victim, but also as the model of cooperation, pointing to examples of its purported benevolent efforts to locate the missing encryption keys and crying, "This is not the conduct of a party trying to conceal or destroy evidence." (Op. Br. 2:22–23.) This is yet another smokescreen Balt erects to distract the Court from its disregard for its obligation to preserve electronic evidence.

First, Balt claims that it "voluntarily turned over" to MVI more 55,000 of MVI's own confidential and propriety documents in the related patent case that Balt had found on its employee laptops. (Op. Br., 2:17–20.) This was not a voluntary act; Balt produced these documents in response to document requests served by MVI seeking confidential MVI documents in Balt's possession. (Hales, ¶8–9.) Second, Balt was not

transparent about how it discovered the stolen MVI documents or where they were located. MVI was required to file a discovery motion in this case to compel Balt to provide this basic information. (Hales, ¶9; Dkts. 145, 146-1.) Third, Balt lied and attempted to minimize the gravity of the situation by claiming MVI documents were found in a single folder on each of the laptops used by Defendants David Ferrera and Jake Le, and nowhere else within Balt's network. (Hales, ¶9.) Forensic evidence uncovered that MVI documents were subsequently found in additional locations on the Ferrera and Le laptops, on other Balt employee laptops, on Balt's current and legacy file servers, in Balt's document control database, and in its cloud storage accounts. (Hales, ¶¶10–11.) Many of the searches that uncovered these MVI documents were ordered by the Court in response to numerous discovery motions filed by MVI.

Balt also claims that it turned the laptops over to Stroz "in working order." (Op. Br. 2:15–21, 3:12–17, 9:17, 10:7–16, 14:14–15.) It is unclear what Balt means by "working order." Regardless, Balt does not address the root problem with this statement, *i.e.,* Balt determined the laptops were purportedly in working order by booting them up the day before Balt provided them to Stroz—something it should not have done. (Dkt. 385-6, p. 2.) As discussed in Section B above, booting a laptop alters the evidence stored on the laptop and should not be performed when laptops are being imaged for forensic examination. (Bandemer, ¶¶4–5.) Stroz did not ask Balt to perform this extra, unnecessary and prejudicial step. (Hales, ¶6.) Balt's outside counsel unilaterally instructed Balt's IT personnel to boot the laptops, without informing either Stroz or MVI. (Hales, ¶¶4, 6–7, Ex. 1, 58:17-59:21.) Ironically, the only legitimate reason to boot the laptops before providing them to Stroz would have been to recover the encryption keys stored on the laptops (Bandemer, ¶5), which Balt failed to do when it alone had the opportunity. The laptops should have been turned over to Stroz "as is," working or not.

Balt also claims that it "include[ed] the encryption keys" when it provided the laptops to Stroz. (Op. Br., 2:14–16, 9:16–18, 10:6–8, 11:11–13.) That, too, is a

misleading statement. To be clear, what Balt is really saying is that the encryption keys were stored ***on the laptops*** themselves and could be retrieved by logging into the laptops with admin credentials. But Balt did not tell Stroz or anyone else that the ***only copies*** of the encryption keys were stored on the laptops, so neither Stroz nor anyone else knew that the encryption keys needed to be retrieved prior to forensic imaging. To the contrary, Balt affirmatively represented to Stroz that it had the encryption keys, and Stroz reasonably relied on that representation in determining how to image the laptops. (Dkt. 386-3, p. 34.)

Balt's reliance on the laptops themselves as the only storage source for the encryption keys defies both logic and best practices in a corporate IT environment. (Bandemer, ¶15.). Balt effectively stored the keys to the safe inside the safe itself, and nowhere else. That is a gross dereliction of duty. Mr. Ang testified that the Tran and Katayama laptops are the only corporate laptops he is personally aware of ***in his entire IT career*** for which the encryption keys had been lost, including hundreds of other laptops at Balt that his IT department has charge of. (Hales, ¶7, Ex. 1, 265:21–266:23; Op. Br. 14:3–4.) This simply does not happen in the real world. (Bandemer, ¶10.)

Further, Balt would have this Court believe that it undertook extensive efforts to locate the encryption keys once it discovered they were lost by searching for them "[o]n its own and in response to requests from MVI." (Op. Br., 14:24–26.) Balt exaggerates the scale of its independent efforts and downplays the extent to which MVI has had to drive the process forward. It was MVI, not Balt, who conferred with its forensics expert and proposed pathways by which the encryption keys might be recovered, and where Balt might search for them. (Dkt. 385-6, pp. 4–23.) Balt did not even retain a forensics expert until ***after*** the damage from the encryption key debacle had already been done. (*Id.*, pp. 4, 18.) That Balt—and its sophisticated IP litigation counsel—chose to navigate the complex forensic process without consulting a forensic expert is beyond explanation. This is particularly perplexing given the ease with which Mr. Massoud is able to provide *post hoc* opinions regarding what should have been done to avoid the

situation Balt created. Mr. Massoud's Monday morning quarterbacking is too little, too late, and is unpersuasive in his efforts to clean up the mess Balt created.

Moreover, Mr. Ang testified in deposition in this case that Balt had not conducted searches for backups of the password database that Balt used (albeit sporadically) for storing laptop encryption keys. (Hales, ¶7, Ex. 1, 172:17–22; Ex. 2, 41:8–43:18.) MVI was forced to file a motion to compel Balt to conduct these searches, but Balt refused to provide any details about the searches it claims to have conducted so MVI could assess the sufficiency of the same. (Hales, ¶12, Ex. 4; Dkts. 338, 356.) One thing is certain, though—Balt did not reach out to any of its former IT personnel to inquire about the encryption keys. Former Balt employee Lincoln Lye procured and likely onboarded the Tran and Katayama laptops. (Hales, ¶¶7, 15, Ex. 1, 53:5–9, 54:17–55:25, 67:20–68:21, 70:21–71:17.) He would be a reasonable person to contact to locate the encryption keys—to determine if they were stored somewhere other than the laptops themselves—but Balt did not bother to ask him. Balt's expert, Mr. Massoud, states that he searched for the encryption keys, but the parameters he used were restrictive and limiting. (*Compare* Dkt. 356, p. 4, *with* Massoud, ¶18.)

The searches Balt undertook for the encryption keys were far from extensive. Indeed, they were nothing more than token efforts to placate MVI (and the Court) and create the illusion of diligence and cooperation where none exists.

F. The Evidence Balt Destroyed is the Data Residing on the Tran and Katayama Laptops, Not the Encryption Keys Within Them

Balt misconstrues the evidence it is accused of spoliating. The critical inquiry is whether Balt caused the destruction of the ***data*** residing on the Tran and Katayama laptops, ***not*** whether Balt lost the encryption keys to access that data. By changing the narrative, Balt hopes to avoid addressing the critical inquiry, and its argument that it cannot have spoliated the data residing on the laptops because it never had the encryption keys for the laptops is another *non sequitur*. (Op. Br., 1:11–13, 7:12–13.) It is also based on an incorrect premise, because Balt's own expert explains that the

encryption keys are located within the laptops themselves, and always have been. (Massoud, ¶¶8, 16.)

The case Balt cites in support of its argument, *Farella v. City of New York*, 2007 WL 193867 (S.D.N.Y. Jan. 25, 2007), has no application here. The spoliated evidence in this case has always been in existence. The spoliated evidence is the data stored on the Tran and Katayama laptops (e.g., technical documents, drawings, spreadsheets, etc.) that is now inaccessible as a result of Balt's affirmative actions. (*See* MVI's opening memorandum, (Dkt. 389-1, 14:4–7, 19:17–25).) Balt conflates the spoliated evidence—that is, the evidence stored on the locked laptops—with the lost encryption keys that are necessary to access that evidence. (Op. Br., 1:11–15.) Its arguments about the timing of when the encryption keys were "lost" are therefore inconsequential and contrived in any event. (Op. Br., 7–8.) Balt argues that it "likely" never made copies of the encryption keys, but even if it did, because the laptops were issued in 2018 before the litigation was foreseeable, those copies were "likely lost long ago." (Op. Br., 7:15–24.) ***The encryption keys are not the spoliated evidence***. The spoliated evidence is the data now locked on the Tran and Katayama laptops, and that data both existed and was accessible until the laptops were locked in April 2022—***after the filing of the litigation***. The encryption keys existed and were also accessible on the laptops until they were locked in April 2022—***after the filing of the litigation***. Moreover, Balt claims that it gave the encryption keys to Stroz, and in the very next breath argues that it lost the encryption keys years before this litigation began. Balt's contradictory arguments undermine its credibility.

In sum, Balt lied to Stroz by representing it had the encryption keys for the laptops when it had made no inquiries to verify if that was true. Had Balt made those inquiries it would have realized it did not have the keys, presumably would have conveyed this information to Stroz, and Stroz could have approached the imaging task differently. Balt could and should have made copies of the encryption keys when it booted the laptops, but again, it did not. Balt could and should have informed Stroz and

MVI that it booted the laptops, but it failed to do that as well. It is the timeline of ***these*** actions and inactions that are relevant to this motion.

G. The Court Has Inherent Power to Fashion Appropriate Sanctions for Evidence Spoliation

Balt cites *Aramark Mgmt., LLC v. Borgquist*, 2021 WL 864067, at *4 (C.D. Cal. Jan. 27, 2021) for the proposition that "this Court's inherent power ***may be*** entirely inapplicable to the present motion" because Rule 37 may be more appropriate when ESI has been spoliated. (Op. Br., 12:2–7 (emphasis added).) However, in *Aramark* Judge Scott "[did] not decide whether the Court could also sanction the parties for spoliation of ESI under its inherent authority." *Id.* District courts have broad inherent and discretionary powers to make appropriate evidentiary rulings in response to spoliation of evidence that match the sanction to the wrongful conduct. *Scalia v. County of Kern*, 2023 WL 2333542, at *3 (E.D. Cal. Mar. 2, 2023) (describing a non-exclusive spectrum of adverse inference instructions available to courts, *e.g.*, that certain facts are deemed admitted and must be accepted as true, a mandatory presumption that the evidence was relevant and unfavorable to the party that that destroyed it, a permissive presumption that the lost evidence is both relevant and favorable to the innocent party, etc.).

Balt's inherent power analysis suffers the same infirmity as its Rule 37 intent analysis because Balt continues to conflate the evidence it is accused of spoliating with the encryption keys. Again, the relevant evidence is ***the data residing on the Tran and Katayama laptops*** that Balt destroyed, ***not the encryption keys*** required to access that data. In addressing the three-part test for the issuance of an adverse inference instruction cited in *Hamilton v. Signature Flight Support Corp.*, 2005 WL 3481423 (N.D. Cal. Dec. 20, 2005), Balt first argues that it had no obligation to preserve the ***encryption keys*** for the Tran and Katayama laptops because the laptops were issued in 2018 before the litigation. (Op. Br., 12:15–18.) Balt does not address its obligation to preserve the ***actual evidence*** at issue—the content of those laptops—which was accessible until the laptops were locked in April 2022.

Regarding the second *Hamilton* element—culpable state of mind—Balt attempts to escape liability by arguing it did not act with bad faith, which Balt claims is required under *America Unites for Kids v. Rousseau*, 985 F.3d 1075 (9th Cir. 2021). (Op. Br. 12:19–25.) For the reasons discussed above in Section B, Balt's conduct ***does*** amount to bad faith. Further, courts have the inherent power to grant adverse inference instructions even when bad faith is not present. *See Scalia*, 2023 WL 2333542, at *4 (granting a permissive adverse inference instruction even though plaintiff did not allege defendant acted in bad faith). In *Scalia*, the court held that it would "instruct the jury of [the] spoliation . . . and permit them to infer that the lost evidence would have been favorable to Plaintiff" because it found the defendant understood its duty to preserve evidence after receiving plaintiff's preservation letters, took no steps during the retention period to "check for and preserve the [evidence] nor note that a technical failure" affected the evidence, and that the loss of the evidence prejudiced the plaintiff. *Id.*, at *4–5. Balt similarly received a preservation notice from MVI, issued its own internal litigation hold memo, affirmatively represented to Stroz that it had the encryption keys for the laptops with conscious disregard for the truth of that representation, and did not note or inform Stroz or MVI that it had booted the laptops. The loss of the Tran and Katayama laptop evidence prejudices MVI because it cannot explore the evidence contained on those laptops, including forensic evidence of the use of MVI documents Tran stole from MVI pertaining to the design, development, manufacture and testing of MVI catheter products.

MVI submits that an adverse inference instruction is warranted here, and requests that the Court exercise its discretion to impose a sanction commensurate with the nature of Balt's destruction of evidence, Balt's culpability and the irreparable prejudice Balt's destruction of evidence has cause to MVI.

III. CONCLUSION

MVI respectfully requests the Court to grant its motion and to issue an adverse inference instruction to the jury, and/or allow MVI to present the facts surrounding Balt's evidence spoliation to the jury.

Dated: April 21, 2023

EVAN FINKEL
CALLIE A. BJURSTROM
MICHAEL S. HORIKAWA
MICHELLE A. HERRERA
CHAZ M. HALES
CHLOE STEPNEY

PILLSBURY WINTHROP SHAW PITTMAN LLP

By /s/ Michelle A. Herrera
Michelle A. Herrera
Attorneys for Plaintiff
MICROVENTION, INC.

[Additional counsel]

Bryan P. Collins (admitted pro hac)
bryan.collins@pillsburylaw.com
PILLSBURY WINTHROP SHAW PITTMAN LLP
1650 Tysons Boulevard, Suite 1400
McLean, VA 22102-4856
Telephone: 703.770.7538
Facsimile: 703.770.7901

CERTIFICATE OF COMPLIANCE

The undersigned, counsel of record for MicroVention, Inc., certifies that this brief contains 6,231 words, which:

__X__ complies with the word limit of L.R. 11-6-1.

_____ complies with the word limit set by court order dated [date].

Executed on April 21, 2023, at San Diego, California.

/s/ Michelle A. Herrera
Michelle A. Herrera