

United States District Court
Southern District of Texas

ENTERED

September 07, 2022

Nathan Ochsner, Clerk

**IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

CHARLES OTIS HERRING,

Plaintiff,

v.

BUC-EE'S LTD. *et al.*,

Defendants.

§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. H-22-330

MEMORANDUM AND OPINION

Charles Otis Herring moves for sanctions under Federal Rule of Civil Procedure 11 against Buc-ee's Ltd., alleging that Buc-ee's's counsel sent Herring an email with two attached files containing malicious code that erased data on Herring's computer and cellphone. (Docket Entry No. 22). Buc-ee's's counsel responded. (Docket Entry No. 25). Based on the motion and response, the record, and the applicable law, the court denies the motion.

Herring's motion follows a discovery dispute with Buc-ee's. In July 2022, Herring learned that Buc-ee's might have had digital surveillance video of him and asked Buc-ee's to produce it. (Docket Entry No. 22 at 2). The next month, after Buc-ee's indicated that it had not yet located the surveillance video, Herring asked Buc-ee's to allow his expert to inspect Buc-ee's's systems and try to locate the surveillance video of Herring. (*Id.* at 3). Buc-ee's refused Herring's request to give his expert access to Buc-ee's's computer system on August 5, 2022. (*Id.*)¹ Buc-ee's sent an email to notify Herring of its decision. That email had two attached files, which Buc-ee's

¹ The merits of the parties' dispute regarding the production of surveillance imagery or Herring's expert's access to Buc-ee's's systems is not before the court on this motion for sanctions. After filing this motion for sanctions, Herring submitted a request for production to Buc-ee's regarding the surveillance imagery. (Docket Entry No. 24).

described as encrypted versions of earlier email communications between Herring and Buc-ee's's counsel. (*Id.*). Herring alleges that when he opened those attachments, a malware program or virus entered his computer and cellphone and erased the information contained on those devices. (*Id.* at 4). He accuses Buc-ee's's counsel of infecting his computer and cellphone, and he seeks sanctions under Rule 11 of the Federal Rules of Civil Procedure.

The first problem with Herring's motion is that he is using the wrong rule. Rule 11 sanctions are for improper statements in filings made with the court. Fed. R. Civ. P. 11(b). This means that "Rule 11 . . . applies *only* where a person files a paper." *Tejero v. Portfolio Recovery Assocs., L.L.C.*, 955 F.3d 453, 458 (5th Cir. 2020) (emphasis added). "Rule 11 does not extend to 'abusive tactics in litigation in respects other than the signing of papers.'" *Id.* (quoting *Thomas v. Capital Sec. Servs., Inc.*, 836 F.2d 866, 875 (5th Cir. 1988) (en banc)). Before filing a motion for sanctions under Rule 11 with the court, the party seeking the sanctions "must" serve the motion on the party against whom sanctions are sought and allow that party an opportunity to cure the improper representation in question. Fed. R. Civ. P. 11(c)(2). As Buc-ee's points out, Herring has not made any allegation that Buc-ee's has violated Rule 11(b) with respect to a filing made with the court. (Docket Entry No. 25 at 2). The subject of Herring's motion is not properly raised in a Rule 11 motion.

The second problem with Herring's motion is that the record fails to provide the necessary support. Herring states that he retained an "IT cybersecurity specialist" to review the attachments that he asserts contained malicious code. (Docket Entry No. 22 at 4). Herring did not submit with his motion a declaration or affidavit from that specialist to substantiate his accusation. Buc-ee's retained a third-party analyst to analyze the attachments. That analyst concluded that the attachments were harmless and so stated in a declaration filed with the court. (Docket Entry No.

25-1 ¶¶ 4–6). The analyst opened the attachments on his computer, but no data was lost or erased. (*Id.* ¶ 4). These attachments did not contain executable code. (*Id.* ¶ 5). The attachments were scanned for viruses, and none were found. (*Id.* ¶ 6). Buc-ee’s’s analyst also noted the presence of computer software on counsel’s law-firm computers designed to prevent the transmission of malicious files to others. (*Id.* at ¶ 7).

Herring sent the court a flash drive that he asserts contains the allegedly infected email attachments. (Docket Entry No. 23). The court lacks the ability or expertise to analyze the contents of the flash drive.

Herring has made a formal request for surveillance video footage to Buc-ee’s, (Docket Entry No. 24), which is conducting a search. (Docket Entry No. 25 at 2 n.1). Buc-ee’s’s conduct to date does not warrant the sanctions Herring seeks. There is simply no evidence to support the conclusion that Buc-ee’s’s counsel deliberately caused the problems Herring had with his cellphone and computer after receiving and opening the email and attachments, other than Herring’s unsubstantiated assertion that they were close in time. That is simply insufficient.

The court denies the motion.

SIGNED on September 7, 2022, at Houston, Texas.



Lee H. Rosenthal
Chief United States District Judge