IN THE SUPREME COURT, STATE OF WYOMING 2022 WY 121

APRIL TERM, A.D. 2022

<u>September 28, 2022</u>

JONATHON TYSON BLAIR,

Appellant (Defendant),

v. S-22-0001

THE STATE OF WYOMING,

Appellee (Plaintiff).

Appeal from the District Court of Sweetwater County The Honorable Suzannah G. Robinson, Judge

Representing Appellant:

Office of the State Public Defender: Diane M. Lozano, State Public Defender; Kirk A. Morgan, Chief Appellate Counsel. Argument by Mr. Morgan.

Representing Appellee:

Bridget L. Hill, Attorney General; Jenny L. Craig, Deputy Attorney General; Joshua C. Eames*, Senior Assistant Attorney General; Catherine M. Mercer**, Assistant Attorney General. Argument by Ms. Mercer.

Before FOX, C.J., and KAUTZ, BOOMGAARDEN, GRAY, and FENN, JJ.

*An Order Allowing Withdrawal of Counsel was entered on August 1, 2022.

**An Order Allowing Withdrawal of Counsel was entered on September 2, 2022.

NOTICE: This opinion is subject to formal revision before publication in Pacific Reporter Third. Readers are requested to notify the Clerk of the Supreme Court, Supreme Court Building, Cheyenne, Wyoming 82002, of any typographical or other formal errors so that correction may be made before final publication in the permanent volume.

BOOMGAARDEN, Justice.

[¶1] Following a jury trial, Jonathon Tyson Blair was convicted of burglary, theft, and property destruction for breaking into his workplace and stealing approximately \$16,000 in cash from the owner's desk. At trial, the district court admitted WiFi records showing only one electronic device—Mr. Blair's Apple iPhone—connected to the business's password protected WiFi network on the night of the burglary. Mr. Blair argues the district court erred by admitting those records under the business records exception to the hearsay rule. We affirm.

ISSUE

[¶2] Did the district court abuse its discretion by admitting WiFi records under the business records exception to the hearsay rule?

FACTS

[¶3] Hager Industries—a machining, welding, and fabrication business in Rock Springs, Wyoming—was burglarized late on the evening of October 17, 2019. The surveillance system recorded someone running toward the building at 10:49 p.m., tilting a camera in the reception area up toward the ceiling at 11:04 p.m., and then running from the building at 11:05 p.m.¹ An office window was broken and approximately \$16,000 in cash was missing from the owner's desk.²

[¶4] In an effort to identify who committed the burglary, Mr. Hager asked Sweetwater Technology Services—the company that managed Hager Industries' password protected WiFi network—whether any devices connected to the WiFi on the night of the burglary. Senior engineer Russell Snody found only one device connected to the WiFi during that timeframe.

[¶5] The device connected at 10:52 p.m. and disconnected at 11:15 p.m. It was an Apple iPhone with a MAC address of e0:89:7e:8e:70:90, and it connected to the WiFi other times in the last 30 days. That the device connected other times caused Mr. Hager to suspect the device belonged to a Hager Industries employee, as employees were provided the WiFi password. On comparing the WiFi records to his employees' timesheets, Mr. Hager

¹ The timestamp on the surveillance videos was approximately 38 minutes behind the actual time. We refer to the actual time.

² The owner, Nathaniel Hager, operated a wholesale CBD supplement business from the same location as Hager Industries. Due to banking issues, it was a cash business. He often kept a small amount of cash in his office desk during the week from sales to family and friends. He stored the CBD business's profits in a bank bag offsite and then brought it to the office at the end of each week to settle accounts with his salesperson. He rarely left the bank bag in his desk overnight but inadvertently did so on October 17.

concluded Mr. Blair—an inspector for Hager Industries—likely committed the burglary. He turned the WiFi records and timesheets over to police.

[¶6] Detective Michelle Hall compared the WiFi records for MAC address e0:89:7e:8e:70:90 to Mr. Blair's timesheets. She concluded the times when the device connected to and disconnected from the WiFi "correlated exactly" to the times when Mr. Blair clocked in and out for work during the last 30 days. Police seized Mr. Blair's Apple iPhone and confirmed its MAC address was e0:89:7e:8e:70:90.

[¶7] Based on this and other circumstantial evidence,³ the State charged Mr. Blair with burglary, theft, and property destruction. He pleaded not guilty to the charges and the case was set for trial.

[¶8] The State listed Sweetwater Technology as a witness in its pretrial memorandum. It noted the witness would testify about managing Hager Industries' WiFi network as well as records for MAC addresses that accessed the WiFi network "on the night of the burglary and when [Mr. Blair] was working." Mr. Blair moved to exclude this witness, reasoning: "testimony regarding the relationship between MAC addresses and the Wi-Fi network would require the witness to express an opinion regarding whether the specific MAC address in question connected to the network at specific times[,]" testimony of this technical nature would require expert testimony, and the witness had not been designated as an expert. The State filed a response clarifying that it did not intend to present testimony about how MAC addresses appear in WiFi connection records. Nor did it intend to ask for an opinion on "whose phone connected or how it connected[.]" Rather, the State intended to introduce WiFi connection records under the business records exception to the hearsay rule, which required no expert. Following a hearing, the court took the matter under advisement for resolution at trial.

[¶9] At trial, Mr. Snody testified that he had worked for Sweetwater Technology for three years and, in his capacity as senior engineer, he managed Hager Industries' WiFi network. Mr. Snody believed Sweetwater Technology set up the network for Hager Industries more

-

³ At 10:17 p.m. on the night of the burglary Mr. Blair sent his girlfriend a text message informing her that he needed to go to Hager Industries to pick up more Tyvek suits for work the following day. However, Tyvek suits had already been delivered to Mr. Blair's worksite that afternoon and Mr. Blair did not have permission to go to Hager Industries after hours. In an interview with police after the burglary, Mr. Blair claimed he never went to Hager Industries on October 17 and insisted there was no reason his phone would have connected to the WiFi that night.

On searching Mr. Blair's home, police found \$2,000 in \$100 bills in a safe in his bedroom and a dirt bike in the living room. Mr. Blair bought the dirt bike shortly after the burglary for \$3,500 in cash. He told his roommate he borrowed money from his boss to buy the bike. However, Mr. Hager denied Mr. Blair's request for a cash advance the week prior to the burglary. Finally, a DNA swab from the broken window "demonstrated the presence of a mixture from which Jonathon Blair [] and additional individuals [could not] be[] excluded as possible contributors."

than three years prior. He explained that the router brand for the network was Cisco Meraki; he and his technicians could remotely manage the network from a password-protected website they referred to as the "Meraki dashboard"; and no one from Hager Industries could access the website.

- [¶10] Using a demonstrative exhibit consisting of screenshots of the website, Mr. Snody explained, step by step, how he navigated the website and what type of information he could find on it. He explained, for example, that the website "holds 30 days['] worth of logs"; he could search for devices that connected to the WiFi network and determine when they connected to and disconnected from the network; and he could download that data to a Microsoft Excel spreadsheet.
- [¶11] Turning to the facts in this case, Mr. Snody testified that, in October 2019, Mr. Hager requested Sweetwater Technology search the WiFi records for any device that connected to the network between 9:00 p.m. and midnight on the night of the burglary. Mr. Snody searched the records, found one device, and sent Mr. Hager a screenshot of what he found. When the State moved to admit the screenshot as Exhibit 35, Mr. Blair objected and requested to voir dire Mr. Snody.
- [¶12] On voir dire, Mr. Snody testified that Mr. Hager had never asked him to conduct this type of search before or since. It was uncommon for clients to request such information. Based on this testimony, Mr. Blair argued the exhibit did not qualify as a business record because it was not a "regularly conducted business activity, and it [was not] the regular practice of the business to keep this record." The State disagreed, maintaining that the underlying data, rather than any document Mr. Snody created for Mr. Hager, constituted the business record. The court overruled Mr. Blair's objection and admitted the exhibit under the business records exception. It proceeded to admit two additional exhibits—Exhibits 36 and 37—as business records over Mr. Blair's objection.
- [¶13] Exhibit 36 contained information about the device that connected to the WiFi on the night of the burglary. It reflected that the device was an Apple iPhone with a MAC address of e0:89:7e:8e:70:90, and the device connected to the WiFi other times between September 24 and October 22. It did not, however, identify who owned the device.
- [¶14] Exhibit 37 contained eight pages of data Mr. Snody downloaded from the website to a Microsoft Excel document and then provided to Mr. Hager. It listed dates and times when the device connected to and disconnected from the WiFi network between September 27 and October 22. Though Mr. Snody acknowledged he could have edited the data contained in the Microsoft Excel document he denied doing so.
- [¶15] Additional witnesses included Detective Hall, who discussed comparing the WiFi records to Mr. Blair's timesheets, as well as Mr. Hager and several law enforcement officers involved in the investigation.

[¶16] The jury found Mr. Blair guilty of burglary, theft, and property destruction. He was convicted of those offenses and sentenced to eight to ten years in prison. This appeal challenging admission of the WiFi records followed.

STANDARD OF REVIEW

[¶17] Because Mr. Blair objected to the WiFi records, we review their admission for abuse of discretion. *Thompson v. State*, 2021 WY 84, ¶ 15, 491 P.3d 1033, 1039 (Wyo. 2021) (citation omitted). The district court abused its discretion if "it could not have reasonably concluded as it did." *Id.* (citation omitted). If the district court abused its discretion by admitting the WiFi records, we must determine whether their admission prejudiced Mr. Blair. *Id.* (citation omitted). The burden to establish abuse of discretion and prejudice is on Mr. Blair. *Kincaid v. State*, 2022 WY 4, ¶¶ 31, 32, 501 P.3d 1257, 1263 (Wyo. 2022) (citations omitted).

DISCUSSION

[¶18] "Hearsay" is defined as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." W.R.E. 801(c).4 "Hearsay statements are generally inadmissible because they are made outside of court and, therefore, presumed to be unreliable." Bruce v. State, 2015 WY 46, ¶ 40, 346 P.3d 909, 923 (Wyo. 2015) (citation omitted); W.R.E. 802. However, there are several exceptions to this rule, including W.R.E. 803(6), which permits the admission of business records. Bruce, ¶ 40, 346 P.3d at 923 (citation omitted); Hodgins v. State, 962 P.2d 153, 157 (Wyo. 1998) ("W.R.E. 803(6) is a firmly rooted exception to the exclusionary hearsay rule. That rule allows business records which meet certain requirements to escape the exclusionary nature of the hearsay rule."). "Where our rules are sufficiently similar to federal rules, we consider federal decisions interpreting them persuasive." Jontra Holdings Pty Ltd v. Gas Sensing Tech. Corp., 2021 WY 17, ¶ 76, 479 P.3d 1222, 1244 (Wyo. 2021) (quoting Mgmt. Nominees, Inc. v. Skowronska, 2019 WY 105, ¶ 31 n.10, 450 P.3d 672, 682 n.10 (Wyo. 2019)). Both our hearsay definition and our business records exception are sufficiently similar to their federal counterpart for federal decisions to be persuasive. Compare W.R.E. 801, and F.R.E. 801; compare W.R.E. 803(6), and F.R.E. 803(6).

[¶19] Mr. Blair contends "the district court erred when it ruled, over defense's objection, that there was sufficient foundation to allow in hearsay evidence under W.R.E. 803(6)." For the first time on appeal, the State argues the WiFi records do not constitute hearsay because they contained computer-generated data. In the alternative, the State argues the records were admissible under the business records exception. Because, as shown below,

⁴ A "statement" is "(1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by him as an assertion." W.R.E. 801(a). "A 'declarant' is a person who makes a statement." W.R.E. 801(b).

4

the State failed to establish the WiFi records contained only computer-generated data, we do not decide whether computer-generated records constitute hearsay. We assume the WiFi records are hearsay and find no abuse of discretion in their admission under the business records exception.

Computer-Generated Records

[¶20] Computer-generated data is often distinguished from computer-stored data, which constitutes hearsay because it consists of information that has been entered into a computer by a person, rather than automatically generated through a computer process. See, e.g., 4 Jones on Evidence § 24:3 (7th ed.), Westlaw (database updated Jan. 2022) ("But if the computer (or other device) is sifting information put into the computer by human beings ('computer-stored' information), and if the record is offered to prove that the facts contained in the record are true, then the record is hearsay, and to be admitted over a hearsay objection the offering party must qualify the record under a hearsay objection." (footnote omitted)); United States v. Ary, 518 F.3d 775, 785–87 (10th Cir. 2008) (addressing admission of a space museum's inventory records, which contained information curators entered into a computer database, and thus constituted hearsay).

[¶21] Some courts hold computer-generated records do not fall within the purview of the hearsay rule because the declarant was not a person and "[a] record created as a result of a computerized or mechanical process cannot lie." State v. Kandutsch, 2011 WI 78, ¶ 61, 336 Wis. 2d 478, 505, 799 N.W.2d 865, 879, superseded by statute on other grounds as stated in In re Commitment of Jones, 2018 WI 44, 381 Wis. 2d 284, 911 N.W.2d 97; see also 4 Jones on Evidence § 24:3 (7th ed.), Westlaw (database updated Jan. 2022) (collecting cases); United States v. Channon, 881 F.3d 806, 810–11 (10th Cir. 2018) (Excel spreadsheets containing machine-generated transaction records fell "outside the purview of" the hearsay rule because the declarant was not a person); *United States v. Hamilton*, 413 F.3d 1138, 1140, 1142–43 (10th Cir. 2005) (header information accompanying pornographic images was not hearsay because it was computer-generated and therefore did not include a "statement" by a "declarant"); United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109-10 (9th Cir. 2015) ("[a] tack placed by the Google Earth program and automatically labeled with GPS coordinates" did not constitute hearsay because it was not an out-of-court statement by a person); but see Baker v. State, 223 Md. App. 750, 762, 117 A.3d 676, 683 (2015) ("To be sure, the view that computer-generated records in general, and phone records in particular, are not hearsay is not shared by all courts." (citing Fry v. State, 885 N.E.2d 742, 747 (Ind. Ct. App. 2008)); United States v. Oliver, 987 F.3d 794, 800 (8th Cir. 2021) ("We are not persuaded by the argument that the markings cannot constitute hearsay simply because they are computer-generated."); Adam Wolfson, Note, "Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay, 104 Mich. L. Rev. 151, 157-58 (2005) (noting that, at least as of 2005, only a minority of states recognized a distinction between computer-stored and computer-generated records for hearsay purposes). We have not ruled on whether

computer-generated data, as opposed to computer-stored data, constitutes hearsay. As noted above, the State brings it to our attention for the first time on appeal.

[¶22] It is well established that we can affirm an evidentiary ruling "on any legal ground appearing in the record." *See, e.g., Martinez v. State*, 2018 WY 147, ¶ 29, 432 P.3d 493, 500 (Wyo. 2018) (citing *Leach v. State*, 2013 WY 139, ¶ 19, 312 P.3d 795, 799 (Wyo. 2013)); *see also Marquess v. State*, 2011 WY 95, ¶ 17, 256 P.3d 506, 512 (Wyo. 2011), *overruled on other grounds by Jones v. State*, 2019 WY 45, 439 P.3d 753 (Wyo. 2019); *Dean v. State*, 2008 WY 124, ¶ 14, 194 P.3d 299, 303 (Wyo. 2008); *Billingsley v. State*, 2003 WY 61, ¶ 9, 69 P.3d 390, 395 (Wyo. 2003). Notably, however, "to overcome a hearsay objection with regard to device-generated information and records, the offering party must both authenticate the record and offer sufficient proof that the record is computer-(or device) generated, rather than based on information inputted by a human source." 4 Jones on Evidence § 24:3 (7th ed.), Westlaw (database updated Jan. 2022). *See also Baker*, 117 A.3d at 682–84 (the Court could not affirm admission of call records on grounds that they did not contain hearsay because there was no evidence establishing they were computer-generated); *Hamilton*, 413 F.3d at 1142 (emphasizing it was "uncontroverted" that the header information was computer-generated).

[¶23] The State asserts Mr. Snody's testimony established the WiFi connection data contained in Exhibits 35, 36, and 37 was automatically created "any time a device connected to or disconnected from Hager Industries' network." The State more specifically directs our attention to the portion of the trial transcript in which Mr. Snody testified to the following: the record showed any device that connected to the WiFi; "[t]he Meraki dashboard holds 30 days['] worth of logs"; to determine how many times a device connected to the WiFi he would click on the client ID and that would bring up a record for the device; and he could determine which websites a device accessed.

[¶24] We conclude neither this nor any other testimony established the WiFi records contained only computer-generated data—that none of the WiFi connection information was entered into a computer by a person. And, as this issue was not presented to the trial court, we cannot say the source of the underlying data contained in the WiFi records was "uncontroverted." *Cf. Hamilton*, 413 F.3d at 1142. Nor can we take judicial notice that the underlying data was computer-generated.⁵ *Cf. Lizarraga-Tirado*, 789 F.3d at 1109

That's not to say machine statements don't present evidentiary concerns. A machine might malfunction, produce inconsistent results or have been tampered with. But such concerns are addressed by the rules of authentication, not hearsay. Authentication requires the proponent of evidence to show that the evidence "is what the proponent claims it is."

6

⁵ That records contain computer-generated data does not guarantee their admission, as such records must still be authenticated and may present other evidentiary issues. As the Ninth Circuit noted in *Lizarraga-Tirado*,

("tak[ing] judicial notice of the fact that the tack was automatically generated by the Google Earth program" because the Court could "access Google Earth and type in the GPS coordinates" and doing so "result[ed] in an identical tack to the one shown on the satellite image admitted at trial"). For these reasons, we cannot affirm on grounds that the WiFi records do not constitute hearsay, and we instead proceed to evaluate their admission under the business records exception.

Business Records Exception

[¶25] W.R.E. 803(6) states:

The following are not excluded by the hearsay rule, even though the declarant is available as a witness:

. . . .

(6) Records of Regularly Conducted Activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by a certification that

Fed.R.Evid. 901(a). A proponent must show that a machine is reliable and correctly calibrated, and that the data put into the machine (here, the GPS coordinates) is accurate. See Washington, 498 F.3d at 231. A specific subsection of the authentication rule allows for authentication of "a process or system" with evidence "describing [the] process or system and showing that it produces an accurate result." Fed.R.Evid. 901(b)(9); see also United States v. Espinal-Almeida, 699 F.3d 588, 612 (1st Cir. 2012) (evaluating whether "marked-up maps generated by Google Earth" were properly authenticated). So when faced with an authentication objection, the proponent of Google-Earth-generated evidence would have to establish Google Earth's reliability and accuracy. That burden could be met, for example, with testimony from a Google Earth programmer or a witness who frequently works with and relies on the program. See Charles Alan Wright & Victor James Gold, Federal Practice & Procedure § 7114 (2000). It could also be met through judicial notice of the program's reliability, as the Advisory Committee Notes specifically contemplate. See id.; Fed.R.Evid. 901 n.9.

789 F.3d at 1110. *See also* Andrea Roth, *Machine Testimony*, 126 Yale L.J. 1972 (2017) (discussing "black box dangers" associated with machine statements).

complies with Rule 902(a)(11) through (14) or with a statute or other court rule permitting certification; or the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit[.]

[¶26] To be admissible under W.R.E. 803(6), the proponent of the memorandum, report, record, or data compilation "must provide testimony by a qualified witness demonstrating" (1) the memorandum, report, record, or data compilation was "made at or near the time" of the event, (2) "by a person with knowledge or [] from information transmitted by a person with knowledge[,]" (3) "if kept in the course of a regularly conducted business activity," and (4) "if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation[.]" W.R.E. 803(6); *Alloway v. RT Cap., Inc.*, 2008 WY 123, ¶ 15, 193 P.3d 713, 718 (Wyo. 2008) (citing *McCone v. State*, 866 P.2d 740, 753 (Wyo. 1993)). Whether the business record exception requirements are met goes to the adequacy of the foundation for their admission. *See Mabe v. State*, 2007 WY 172, ¶ 12, 169 P.3d 870, 873 (Wyo. 2007) (noting that "[f]oundation, in this context, related to whether the invoices qualified as business records"); *see also Schmidt v. State*, 2017 WY 101, ¶¶ 26–27, 401 P.3d 868, 878 (Wyo. 2017) (discussing the foundation requirements for admission of a statement under W.R.E. 803(4)).

[¶27] Mr. Blair argues the State failed to establish any of these foundational requirements for admission of Exhibits 35, 36, and 37.6 The State responds that we should not consider any arguments concerning foundation that Mr. Blair did not raise in the district court. We agree that a party may not raise additional challenges to foundation for the first time on appeal.

[¶28] "We have observed that it is unfair for a party to challenge foundation for the first time on appeal because it deprives the offering party of the opportunity to correct any deficiency in the proof." *Neidlinger v. State*, 2021 WY 39, ¶ 26, 482 P.3d 337, 345 (Wyo. 2021) (citing *Mayhew v. State*, 2019 WY 38, ¶ 53, 438 P.3d 617, 634 (Wyo. 2019)). "For this reason, we have held that 'objections based on the adequacy of foundation must be made when evidence is offered, and the failure to make a timely objection will preclude appellate review." *Id.* (quoting *Putnam v. State*, 2020 WY 133, ¶ 22 n.2, 474 P.3d 613, 619 n.2 (Wyo. 2020)). Though these cases involved situations where the defendant failed to lodge any foundation challenge in the district court, *id.* ¶ 26, 482 P.3d at 345; *Mayhew*,

⁶ "The party objecting to the admission of a business record has the burden of establishing that a lack of trustworthiness should keep the document out of evidence." *Black Diamond Energy, Inc. v. Encana Oil & Gas (USA) Inc.*, 2014 WY 64, ¶ 51, 326 P.3d 904, 917 (Wyo. 2014) (citing *Mabe*, ¶ 16, 169 P.3d at 874).

¶ 53, 438 P.3d at 634; *Putnam*, ¶ 22 n.2, 474 P.3d at 619 n.2, the same principles apply to this case.

[¶29] Mr. Blair's foundation challenge was narrow in the district court. He argued the documents admitted as exhibits were not kept in the regular course of a regularly conducted business activity for Sweetwater Technology and it was not the "regular practice" to create the documents. His argument is much broader than that on appeal. He adds that the documents were "not 'made at or near the time' of the incident by Sweetwater Technology[,]" the documents were not produced by someone from Sweetwater Technology "with knowledge' of the matters recorded[,]" and Mr. Snody could not lay the foundation for the exhibits because they were Cisco Meraki's records, not Sweetwater Technology's.

[¶30] Mr. Blair may not raise these new challenges to foundation for the first time on appeal because it deprives the State the opportunity to correct any deficiency in proof. *See Neidlinger*, ¶ 26, 482 P.3d at 345. We therefore limit our consideration to the narrow foundation issue he raised in the district court.

[¶31] Mr. Blair argues the WiFi documents admitted as Exhibits 35, 36, and 37 were not admissible under the business records exception because they were not kept in the course of a regularly conducted business activity nor was it the regular practice to keep such documents. To support this argument, he directs our attention to Mr. Snody's testimony that Mr. Hager never asked him for information about when devices connected to the WiFi network before or since the October 2019 request. But this argument misses the mark because the relevant question is not whether it was Sweetwater Technology's regular practice to create the documents that were introduced as exhibits. The relevant question is whether Sweetwater Technology kept the data reflected in those documents as a matter of regular practice. See, e.g., United States v. Keck, 643 F.3d 789, 797 (10th Cir. 2011) ("In the context of electronically-stored data, the business record is the datum itself, not the format in which it is printed out for trial or other purposes."); Potamkin Cadillac Corp. v. B.R.I. Coverage Corp., 38 F.3d 627, 632 (2d Cir. 1994) ("A business record may include data stored electronically on computers and later printed out for presentation in court, so long as the original computer data compilation was prepared pursuant to a business duty in accordance with regular business practice") (citation and internal quotations omitted)). Based on Mr. Snody's testimony about managing Hager Industries' WiFi network and accessing the information contained on the "Meraki dashboard" the district court could reasonably conclude it did. Therefore, the district court did not abuse its discretion by admitting Exhibits 35, 36, and 37 under W.R.E. 803(6), the business records exception to the hearsay rule.

[¶32] Affirmed.