North Carolina Criminal Law Blog

July 24, 2025

A New Way to Authenticate Video? State v. Windseth and the Business Records Exception

Daniel Spiegel

Special thanks to Sloan Godbey, Summer Law Fellow at UNC SOG, for their significant contributions to this post.

In March of last year, I did a thorough review of North Carolina cases addressing the authentication of surveillance video. I created a chart to understand what ingredients are adequate (and inadequate) to lay a foundation. That chart can be found **here**, and the related blog **here**.

However, a case came down in March of this year that raises significant questions about how video is authenticated, or at least introduces a new potential avenue for authenticating video. I'm afraid my cherished chart may soon be of limited utility. But such is the way the law develops!

The Case

The case is ***State v. Windseth***, COA24-718, ___ N.C. App. ___ (March 19, 2025). The underlying facts, which involved an investigation into the whereabouts of the defendant's mother leading to charges against the defendant for fraudulent use of his mother's bank card, are not of great import to our evidentiary inquiry. The key points for our purposes are that in the course of trying to locate the defendant's mother, the lead investigator requested information from Wells Fargo, and the bank produced a variety of documents and videos. Slip op. 2-3. The videos originated from ATM surveillance cameras and appeared to show the defendant using his mother's bank card.

At trial, the State attempted to introduce still-shots from the ATM videos through a method I have not seen before in North Carolina caselaw. The State admitted

the videos under the business records exception to the hearsay rule pursuant to Rule 803(6). The State relied on the affidavit received from Wells Fargo containing standard attestations that the records (1) were prepared by Wells Fargo personnel in the ordinary course of business at or near the time of the events described, (2) were made by employees "with knowledge," and (3) were "true and correct" copies (Jonathan Holbrook blogged about authenticating business records by affidavit **here**; also note that a recent change to the law allows for authentication through a signed statement made under penalty of perjury *or* a notarized affidavit, *see State v. Hollis*, 295 N.C. App. 224, 232 (2024); S.L. 2023-151; N.C. Gen. Stat. 8C-1, Rule 803(6) (2024)).

This is a significant development in the law of video authentication. Prior to *Windseth*, no North Carolina case approved of this method of authentication. Although the formula is not exact (hence the **chart**), earlier caselaw held that the proponent of video evidence must elicit testimony to the effect that the recording equipment was in good working order and generally reliable, or that the video footage introduced in court is the same as that viewed by the witness on the recording equipment shortly after the incident in question. This testimony establishes that the surveillance video reliably captured real-life events.

Is such testimony, designed to assure the trial judge as gatekeeper that the video recording technology can be trusted, no longer necessary? My previous **post**, spurred by the *Jones* case in which video was introduced through an officer rather than a homeowner or store manager, observed a trend toward relaxing the requirements to authenticate a video. But *Windseth* goes a step further in that the authenticating witness disappears completely and is replaced by a written statement. Although the statement in *Windseth* contained an attestation that the video was "true and correct," evidence establishing that the video equipment was in good working order is noticeably absent.

Challengers to this method of authentication can argue that *Windseth* does not explicitly hold that video can be authenticated as a business record, as the Court of Appeals stressed that the defendant only challenged the still-shots at trial, not the videos themselves. The *Windseth* court did not engage deeply with the question of whether this method of authenticating video was proper, as it was instead focused on the secondary question of whether the still-shots, extracted from "unobjected security video," were properly introduced into evidence. This question the court answered in the affirmative without too much trouble, finding an analogous fact pattern in *State v. Jackson*, 229 N.C. App. 644 (2013). *Jackson* involved the introduction of a video file plotting data from an electronic

monitoring device after the device and the data were introduced without objection. If the holding of *Windseth* is limited to admission of the still-shots and the conclusion that the videos were properly authenticated is mere dicta, then it is perhaps not as significant a development as it appears on first blush.

Video as Business Record in Other States

However, a survey of other jurisdictions shows that numerous courts have allowed video to be introduced as a business record, and no appellate court appears to have expressly held that the method is improper.

In *Dep't of Pub. Safety & Corr. Servs. v. Cole*, 672 A.2d 1115 (1996), the Court of Appeals of Maryland addressed the question at length and concluded that surveillance video can properly be admitted as a business record under Rule 803(6). Although the case involved review of an administrative hearing with relaxed evidentiary requirements, the court held that the videotape in question would have been admissible even if the proceeding had been judicial in nature.

Subsequently, in an unpublished opinion, the Court of Special Appeals of Maryland relied on *Cole* to hold that video evidence was properly admitted in a criminal case as a self-authenticating business record, despite the absence of a live foundation witness. *See Jeffries v. State*, No. 2993, Sept. Term, 2018, 2019 WL 5213008 (Md. Ct. Spec. App. Oct. 16, 2019) (unpublished). The *Jeffries* court explicitly stated that the business records exception does not require evidence regarding "the process used, the manner of operation of the cameras, the reliability of authenticity of the images or the chain of custody of the pictures." *Id* at *5.

The Fourth Circuit of the Court of Appeal of Louisiana addressed the question as a matter of first impression just last year. *See State v. Davis*, 400 So. 3d 260 (La. 2024). The case came up on the State's interlocutory appeal after the trial court ruled that the gas station surveillance video in question could not be admitted under the business records exception. The appellate court reversed, concluding that the video did qualify as a business record and could properly be admitted through self-authentication under Rule 902.

Another example is *United States v. Clotaire*, 963 F.3d 1288 (11th Cir. 2020), on which the *Windseth* Court (and the *Davis* Court) relied. In *Clotaire*, the defendant was caught on camera repeatedly withdrawing funds from various ATMs with fraudulent debit cards he had opened in the victims' names. *Id*. at 1292. As in *Windseth*, the court considered whether there was an evidentiary problem with

extracting still photos from video footage and concluded that there was not. *Id.* at 1293. However, as was again the case in *Windseth*, "no one contest[ed]" whether the video itself could be introduced as a business record, so the Federal Circuit court did not squarely address the question. *Id.* The court seemed to assume that it was not an issue.

Although the South Dakota Supreme Court case of *State v. Turner*, 18 N.W.3d 673, 686-88 (S. D. 2025), did not hold that it was improper for video to be admitted through the business records exception, it is worth a mention. The court held that the video was not properly introduced as a business record under Rule 803(6) because the authenticating witness, a police officer, was not an appropriate witness "with knowledge" (compare this case with the ***Jones* case**). Though the police officer in *Turner* was in the room when a still photo from a traffic camera system was printed, the officer could not establish how the date and time were affixed to the particular photograph, nor the accuracy of the date and time stamp, and the timing was crucial to the case. The court made a distinction between the authentication requirements and the business records requirements in coming to its conclusion. *Turner* is an example of how courts may still require some minimal level of familiarity with the workings of the recording device before allowing video evidence to be introduced as a business record.

Objections

When one imagines a business record, an image of a paper document in a file folder comes to mind, or perhaps a digital file such as a spreadsheet. Is footage from a surveillance video camera akin to such a document? The courts from the multi-jurisdiction survey above do not seem troubled by including video footage in the business records category, finding such footage implicitly trustworthy. This is the case despite new concerns about AI-manipulated video discussed in the **blog** referenced above.

What if the video recording is silent? Can it be admitted through the business records exception to the hearsay rule when the video doesn't even contain any hearsay? The *Jeffries* court did not see a problem with this, collapsing the analysis into authentication and finding no authority that a business record must contain hearsay in order to be self-authenticating. *See* Maryland's Rule 902 (note that **North Carolina's Rule 902** differs from Maryland's Rule 902, as discussed below).

What of the requirement of 803(6) that the witness have "knowledge?" The written business records declaration in *Windseth* did not establish what if

anything the witness knew about whether the video was in good working order. How much "knowledge" is necessary on the part of the witness? Perhaps not much, when one reflects on the average technical knowledge of a homeowner or store manager. But whereas the testifying homeowner or store manager may at least have familiarity with the videos produced by the surveillance system and be able to establish that the system previously produced accurate recordings of real events, it seems unlikely that the Wells Fargo employee who signed the business records declaration in *Windseth*, probably in an off-site corporate office somewhere, knew anything about the reliability of the particular ATM camera that captured the defendant's face.

Previous North Carolina decisions addressing foundation for video, such as *State v. Snead*, 368 N.C. 811 (2016), and *State v. Jones*, 288 N.C. App. 175 (2023), cited to **Rule 901(a) and 901(b)(9)** when discussing authentication of video evidence. Rule 901(a) states that an item can be authenticated with "evidence sufficient to support a finding that the matter in question is what its proponent claims;" *see also State v. Ford*, 245 N.C. App. 510 (2016) (the "burden to authenticate under Rule 901 is not high – only a *prima facie* showing is required"). But the traditional method of video authentication under Rule 901(b)(9) calls for evidence "describing a process or system used to produce a result and showing that the process or system produces an accurate result." The *Windseth* Court did not address the 901(b)(9) method (although it's important to note that this is only one of several "illustrative" methods listed in subsection (b), and Rule 803(6) also refers to "authentication").

The out-of-state cases discussed above invoke Rule 902 (self-authentication) along with Rule 803(6). Previous North Carolina cases do not rely on Rule 902, and North Carolina's version of 902 does not contain a category that applies to surveillance video. Note that Federal Rule 902 and other states' Rule 902 differs from North Carolina Rule 902 in potentially important respects. The Louisiana version makes reference to 803(6), the Maryland version makes reference to both 803(6) and, after a 2021 revision, to electronic records, and the Federal version also refers to both 803(6) and electronic records, whereas the North Carolina version refers to neither.

The dissent in the *Cole* case out of Maryland, in disagreeing that a proper foundation had been laid for the surveillance video, complained that no testimony established that the camcorder was working properly, no testimony spoke to the "accuracy of the process" that produced the videotape, and no testimony addressed whether the videotape may have been tampered with or altered. The

dissent cited to various treatises on evidence (McCormick and Wigmore) discussing the reliability of products of scientific processes. *Cole*, 672 A.2d at 1125-27. But this language from the 1996 opinion may be outdated given how common video footage is today. Have we moved past the point of requiring someone to testify that a video recording system is working properly?

Conclusion

If the business records exception is in fact a viable way to authenticate video, it could potentially save the state the trouble of subpoenaing reluctant or hard-to-find witnesses in order to present crucial video evidence to the jury. However, obtaining an affidavit or sworn statement may prove difficult in some cases. Not every business has a custodian of records readily available to produce an affidavit or declaration. And furthermore, *Snead* and *Jones* have not been overruled and are still good law in North Carolina. Given the objections that may be made, you might not want to throw away the **chart** just yet.

I'd love to hear from you if you have thoughts on these developments. You can drop a comment or email me at spiegel@sog.unc.edu.