

**UNITED STATES NAVY-MARINE CORPS
COURT OF CRIMINAL APPEALS
WASHINGTON, D.C.**

**Before
J.A. MAKSYM, J.R. PERLAK, B.L. PAYTON-O'BRIEN
Appellate Military Judges**

UNITED STATES OF AMERICA

v.

**LLOYD G. FISHER
AVIATION STRUCTURAL MECHANIC AIRMAN (E-3), U.S. NAVY**

**NMCCA 201000287
GENERAL COURT-MARTIAL**

Sentence Adjudged: 22 January 2010.

Military Judge: CAPT John K. Waits, JAGC, USN.

Convening Authority: Commander, Navy Region Southeast,
Naval Air Station, Jacksonville, FL.

Staff Judge Advocate's Recommendation: CDR F.J. Yuzon,
JAGC, USN.

For Appellant: Capt Jeffrey R. Liebenguth, USMC.

For Appellee: Capt Samuel C. Moore, USMC.

30 June 2011

OPINION OF THE COURT

**IN ACCORDANCE WITH RULE 18.2, NMCCA RULES OF PRACTICE AND PROCEDURE, THIS
OPINION DOES NOT SERVE AS PRECEDENT.**

PAYTON-O'BRIEN, Judge:

The appellant was tried by a general court-martial composed of officer and enlisted members. Contrary to his pleas, he was convicted of one specification each of wrongful appropriation and larceny, and four specifications of housebreaking, in violation of Articles 121 and 130, Uniform Code of Military Justice, 10 U.S.C. §§ 921 and 930. The appellant was sentenced to restriction for 30 days, forfeiture of \$750.00 pay per month for one month, reduction to pay grade E-1, and a bad-conduct discharge. The convening authority approved the sentence as adjudged, and except for the bad-conduct discharge, ordered it executed.

On appeal, in his sole assignment of error,¹ the appellant asserts that the military judge erred in admitting into evidence, over defense objection, computer-generated printouts marked as Prosecution Exhibits 10-17.

After careful examination of the record of trial and the parties' pleadings, we conclude that the findings and the sentence are correct in law and fact and that no error materially prejudicial to the substantial rights of the appellant was committed. Arts. 59(a) and 66(c), UCMJ.

Factual Background

In July 2009, the appellant lived in the Bachelor Enlisted Quarters (BEQ) aboard Naval Station Mayport, Florida. Over the Independence Day weekend, a number of break-ins and thefts occurred in the BEQ, and the appellant became the lead suspect almost immediately upon the discovery of the crimes.

Shortly after midnight on 4 July 2009, the first larceny victim, Aviation Machinist's Mate Airman Apprentice (ADAN) E, reported to BEQ front desk personnel that a laptop computer, webcam and power cord had been stolen from his BEQ room while he was away. Upon learning of the theft, the front desk clerk, Ship's Serviceman Second Class (SH2) Christopher Taylor, took a device commonly known to BEQ personnel as the "black box" to the victim's room, plugged it into the electronic door lock, and "read" the "Openings" information from that particular door lock into the "black box." By reading the door lock in this fashion, SH2 Taylor discovered that a BEQ manager's master keycard had been used to access the victim's room during the evening that the items were stolen from the room.² Later that morning, when the shifts changed, SH2 Taylor passed down the reported theft and the information about the "black box" reading to the oncoming BEQ front desk clerk, SH2 Carlos Valdez.³

In an effort to determine why a BEQ manager's master keycard had been used to access a resident's room, SH2 Valdez made telephonic contact with the BEQ manager who owned the master key card, SH2 Kendrish Lissade, who was at that time off duty at his residence. SH2 Lissade related that he believed his keycard

¹ TO INTRODUCE COMPUTER-GENERATED PRINT-OUTS INTO EVIDENCE, THE PROPONENT MUST: (1) AUTHENTICATE THE EXHIBITS AS THE PRINT-OUTS THEY PURPORT TO BE AND, (2) AUTHENTICATE THE PROCESS BY WHICH THEY WERE PREPARED TO SHOW THAT IT PRODUCES ACCURATE PRINT-OUTS. DID THE MILITARY JUDGE ABUSE HIS DISCRETION WHEN, OVER DEFENSE OBJECTION, HE ADMITTED COMPUTER-GENERATED PRINT-OUTS OF ELECTRONIC-LOCK DATA WHERE THE EVIDENCE DID NOT ESTABLISH THE AUTHENTICITY OF THE PRINT-OUTS OR THE PROCESS BY WHICH THEY WERE CREATED?

² A building manager's keycard can access any room in the BEQ.

³ At the time of these offenses, SH2 Valdez was assigned as Building Manager for the Mayport BEQ, but served on a rotating basis as front desk clerk. He had various duties, including room check-ins, room inspections, guest control, and making and issuing room keys.

should be in the specific lockbox designated for the BEQ managers' master keycards. But, after SH2 Valdez could not locate SH2 Lissade's master keycard in the lockbox, he again contacted SH2 Lissade, and learned from SH2 Lissade that he had issued a temporary key card the night before to a BEQ resident locked out of his room, and he believed he may have mistakenly mixed up the master keycard and the temporary card, thereby giving the master keycard to the resident locked out of his room. SH2 Lissade provided enough information to SH2 Valdez about the resident's possible room number, enabling SH2 Valdez to utilize the "black box" to conduct room lock readings. As a result of these subsequent "black box" readings, SH2 Valdez learned that the appellant's room was accessed several times with SH2 Lissade's building manager keycard the night before.

Concerned about building security, SH2 Valdez went to the appellant's room in an effort to retrieve the building manager's keycard. However, SH2 Valdez was not able to find the appellant until the next day, 5 July 2009. When SH2 Valdez went to the appellant's room, he found the appellant in the room and asked for the return of the master key and the laptop.⁴ The appellant responded, "Yeah, yeah," and commenced looking through the dresser drawers. Ultimately, the appellant turned over the master key to SH2 Valdez, which he had in the pocket of his shorts.⁵ The appellant also gave SH2 Valdez the laptop belonging to ADAN E, which he had in the back seat of his car, the web camera, which he had in the trunk of his car, and the power cord, which he retrieved from another BEQ resident to whom he had given the cord.⁶ The appellant asked for the identity of the laptop's owner, because he wanted to apologize, but SH2 Valdez refused to give that information to him.⁷

On 6 July 2009, after other BEQ residents reported thefts of personal property, security was contacted, and the Criminal Investigative Division (CID) was assigned to investigate the larceny of ADAN E's laptop computer as well as the other BEQ larcenies. The appellant was brought in for questioning and although he provided multiple conflicting accounts of the events over that weekend, he ultimately confessed to wrongfully entering another person's barracks room and stealing a laptop, power cord and web camera.⁸

⁴ Record at 700.

⁵ *Id.* at 704-05.

⁶ *Id.* at 708, 714, and 716.

⁷ *Id.* at 709-11.

⁸ Prosecution Exhibit 22. The appellant does not contest on appeal the admissibility of his statements to SH2 Valdez or the property retrieved by SH2 Valdez, although he had filed a motion to suppress both at trial, which was denied by the military judge. Record at 235-48; AE IV. We hold that the military judge's factual findings in this case are well-supported by the

During the investigation, SH2 Valdez obtained "black box" readings from the various BEQ rooms which had been broken into and items stolen. "Black box" readings indicate which room was accessed, what electronic key cards were used to enter a particular room, and on what dates the room was accessed. The "black box" readings were reduced to computer-generated spreadsheets, saved to a floppy disc and the disc given to Master-at-Arms Second Class (MA2) Elizabeth Luna of CID. MA2 Luna printed the documents from the floppy disc. During a pretrial Article 39(a), UCMJ, session, the Government attempted to pre-admit the computer generated printouts. PE 10-17. During these sessions of court, the Government called upon SH2 Valdez to testify concerning the procedures he utilized with the "black box" to obtain the electronic lock data, and MA2 Luna to testify how she obtained the electronic lock data and printed out the data. The military judge thereafter admitted Prosecution Exhibits 10-17 into evidence over a defense objection.

Authenticity of the "Black Box" Computer-Generated Printouts

The appellant alleges that the Government failed to properly authenticate the computer-generated printouts of the "black box" data admitted into evidence. We review a military judge's decision to admit or exclude evidence for an abuse of discretion. *United States v. Jenkins*, 63 M.J. 426, 428 (C.A.A.F. 2006). The abuse of discretion standard is a strict one, calling for more than a mere difference of opinion. *United States v. McElhaney*, 54 M.J. 120, 130 (C.A.A.F. 2000). The challenged action must be "arbitrary, fanciful, clearly unreasonable," or "clearly erroneous." *United States v. Miller*, 46 M.J. 63, 65 (C.A.A.F. 1997) (internal quotation marks and citations omitted). In this instance, we hold that the military judge did not abuse his discretion in admitting the computer generated printouts marked as Prosecution Exhibits 10-17.

As a general rule, authentication as a condition precedent to admissibility "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." MILITARY RULE OF EVIDENCE 901(a), MANUAL FOR COURTS-MARTIAL, UNITED STATES (2008 ed.). More specific to computer-generated print-outs, a proponent of such evidence must authenticate the exhibit as the print-out it purports to be, as well as authenticate the process by which it was prepared to show that print-outs are produced which accurately reflect the input data. *United States v. Duncan*, 30 M.J. 1284, 1288 (N.M.C.M.R. 1990).

Prior to the admission of the PE 10-17 into evidence, SH2 Valdez testified at the Article 39(a) session that in July 2009 he was familiar with the use of the "black box," having used it

evidence and that, based on those factual findings, the military judge did not commit legal error in refusing to grant the appellant's motion to suppress.

"hundreds of times" previous to the incident at bar,⁹ as he had been assigned to the BEQ for 18-24 months. He was very familiar with the Onity computer system, which was used for encoding the keycards for BEQ rooms, as he had programmed keys "thousands of times."¹⁰ He explained when using the "black box" to retrieve lock data, he would attach the box to the lock via a cord similar to an electrical cord, elect the "read" function, and download the data from the lock. Once the data dump from the electronic lock to the "black box" was completed, the "black box" would be detached from the lock and thereafter attached to the Onity computer. The Onity computer is specifically used for the keycard system in place at the Mayport BEQ.¹¹ The Onity computer screen displays in spreadsheet form the specific lock data which had just been retrieved from the electronic lock during the data dump.¹² However, because the Onity computer has no capability to print the data, the user must save the data to a disc, in order for the data to be subsequently printed.¹³

After CID commenced this investigation, SH2 Valdez was ordered by his supervising chief petty officer to conduct "black box" lock readings of approximately seven or eight BEQ room locks and to download the data onto a disc.¹⁴ After SH2 Valdez conducted the readings as instructed, he saved the data to a disc, and provided it to his supervisor. SH2 Valdez testified that the data that had been downloaded from the electronic locks and displayed onto the Onity computer screen was duplicated in almost-exact form onto the discs, as the data cannot be altered in the Onity computer.¹⁵ The only exception was the room or lock number heading, which was present on the Onity computer screen, but was not present in the computer generated printout. The room or lock number heading does not duplicate onto the printout.

MA2 Luna, the CID investigating detective, had watched "black box" readings at the BEQ, readings both conducted by SH2 Valdez and by other BEQ personnel. She testified at the Article 39(a) session to a process similar to that testified by SH2 Valdez. MA2 Luna had identified certain BEQ room numbers for which she wanted "black box" readings (based upon the reports of theft), and once the readings were completed, she went to the BEQ front desk.¹⁶ The "black box" was plugged into the Onity computer

⁹ Record at 514.

¹⁰ *Id.* at 549.

¹¹ *Id.* at 517.

¹² *Id.* at 532-33.

¹³ *Id.* at 534.

¹⁴ *Id.* at 580-81.

¹⁵ *Id.* at 303, 305, 584-86.

¹⁶ *Id.* at 609.

and MA2 Luna observed the spreadsheets on the computer screen.¹⁷ She saw a BEQ room number at the top of the spreadsheets for the "black box" readings.¹⁸ The information was saved onto a disc and the disc was provided to her. She thereafter printed the electronic lock data saved to the disc using another computer. She did not alter the data on the disc and did not witness anyone else alter the data on the screen before she printed the information.¹⁹ She testified that the information she saw on the screen was the same information that was printed out. MA2 Luna retained the disc at all times during the investigation, unless she had passed it back to BEQ personnel to save more electronic lock data in response to her requests.

SH2 Valdez identified PE 10-17 as Onity computer generated print-outs from the "black box" readings of the electronic door data from various BEQ rooms that were part of this investigation. MA2 Luna also identified the printouts in PE 10-17 as the same documents she obtained during the investigation. To aid her in her investigation, she wrote either the case number or the victim's name at the top of PE 11-17 (PE 10 is a printout for the appellant's BEQ room). At the conclusion of the Article 39(a) session, the military judge overruled the defense authenticity objection, and admitted PE 10-17.²⁰

The military judge, recognizing that there had been some conflicts in the testimony between the two government witnesses at the Article 39(a) session regarding the details of the printouts and the alleged broken chain of custody of the computer disc, determined by a preponderance of the evidence, "that the witnesses do recognize these printouts, how they recognize these printouts, and how they pertain to certain doors. They've explained what these printouts show [and] how they know what they show" ²¹ The military judge took into account the conflicts of the testimony, ruling that "this goes to the weight rather than the admissibility of the evidence."²² The military judge's findings were amply supported by the evidence.

In reaching our decision today, we note that at trial the Government called SH2 Valdez to authenticate PE 10-17 before the members. SH2 Valdez testified again extensively about the Onity key card system, the "black box" procedures, and his role and responsibilities as a member of the BEQ staff in utilizing those systems. The appellant's trial defense counsel conducted a

¹⁷ *Id.* at 604.

¹⁸ *Id.* at 606.

¹⁹ *Id.* at 611.

²⁰ *Id.* at 639, 647.

²¹ *Id.* at 647.

²² *Id.*

thorough cross-examination of SH2 Valdez. The members asked numerous questions about the exhibits, and the military judge even recalled SH2 Valdez to answer members' questions specific to the electronic door readings and the printouts. While there were some minor inconsistencies between SH2 Valdez's earlier testimony at the Article 39(a) session and his testimony in front of members, he demonstrated a detailed understanding of the key card system and the "black box", sufficient that we harbor no doubt that he was completely knowledgeable about the system in question having been a consistent and constant user of both. Although not an expert, SH2 Valdez's testimony established that the system was running "error-free" over a suitable period of time. *Duncan*, 30 M.J. at 1289. Furthermore, given that the electronic lock data as shown on the Onity computer screen cannot be manipulated, and according to witness testimony was never manipulated in this case, the data on the computer disc is "computer-generated," not "computer-stored" data, as the appellant contends. The military judge ruled that the data in PE 10-17 was computer-generated, not computer stored, and therefore was not hearsay. Based upon the facts of this case, we agree with the military judge that the data was not hearsay and no hearsay exception was required for their admission. *Id.* at 1288.

Taking into account this record as a whole, the testimony of SH2 Valdez and MA2 Luna were sufficient to authenticate PE 10-17. As the military judge determined, the conflicts in the evidence was a matter that went to the weight the fact-finder might give the evidence, and not to its admissibility.²³ See *United States Blanchard*, 48 M.J. 306, 311 (C.A.A.F. 1998).

We conclude that the military judge's ruling was not clearly erroneous, his conclusions correct, and he did not abuse his discretion in finding that PE 10-17 were properly authenticated under MIL. R. EVID. 901(a). Accordingly, the appellant's assignment of error must fail.

Conclusion

The findings and the sentence are affirmed.

Senior Judge MAKSYM and Judge PERLAK concur.

For the Court

R.H. TROIDL
Clerk of Court

²³ The appellant contends that someone must have altered the data on the computer disc due to the presence of different fonts, yet there was no evidence presented at trial that anyone altered the data (or the fonts) contained therein. In the absence of evidence, we refuse to speculate post-trial as to the meaning of different fonts.