# CONTINUATION IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Evan Alkema, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this continuation in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property (two electronic devices) which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since January 2025. I am currently assigned to the Detroit Field Office, Kalamazoo Resident Agency. Prior to my employment with the FBI, I was a Trooper and Detective Trooper for the Michigan State Police (MSP) for approximately 10 years. During my employment with MSP, I investigated numerous cases involving theft of valuable items.

3. This continuation is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set forth in this continuation are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses, including consultations with the FBI Art Crime Team.

## IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The devices to be searched are (1) a black Google wireless telephone, and (2) a gray Hewlett Packard laptop computer which belonged to MIKOLAI STASIULEWICZ, who is deceased, hereafter the Devices. The Devices are in secure custody at the Federal Bureau of Investigation Detroit Division – Grand Rapids Resident Agency located at 330 Ionia Avenue, Northwest, Grand Rapids, Michigan.

5. The applied for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

## PROBABLE CAUSE

6. Based on the facts set forth in this affidavit, I submit there is probable cause to believe that violations of 18 U.S.C. §§ 668, 2314, and 371, hereinafter the Subject Offenses, have been committed by MIKOLAI STASIULEWICZ and persons yet unknown. There is also probable cause to believe the information described in Attachment B will constitute evidence of these criminal violations, and will lead to evidence of the commission of these offenses.

7. 18 U.S.C. § 668 (theft of major artwork) makes it a felony to steal an object of cultural heritage from a museum. A "museum" is defined to include any organized, permanent institution established for educational or aesthetic purposes, that has a professional staff, and exhibits tangible objects to the public. An "object of cultural heritage" is an object that is over 100 years old and worth more than $5,000, or is worth more than $100,000. 18 U.S.C. § 2314 (transportation of stolen property)

makes it a felony to knowingly transport stolen goods worth more than $5,000 in interstate or foreign commerce. 18 U.S.C. § 371 makes it a crime to conspire to commit any federal offense, including §§ 668 and 2314 described above.

## I. Overview

8. On July 8, 2026, the FBI became aware of and investigated two separate art thefts in Kalamazoo and Kent counties, in the Western District of Michigan. The first incident, which occurred on June 23, 2026, was the theft of *"Red, Blue, Yellow*" – a color lithograph by artist Ellsworth Kelly purchased by Western Michigan University (WMU) in 1987, which was publicly displayed in their art collection. This work of art is insured by WMU for $10,000.00. The second incident, which occurred on July 2, 2026, was the theft of *"The Sudarium Held by One Angel"* an etching by artist Albrecht Dürer produced in the year 1516, which was part of collection of the Grand Rapids Art Museum (GRAM). This work of art is valued between $10,000.00 to $20,000.00. The FBI's investigation thus far has identified the subject responsible for these thefts as MIKOLAI STASIULEWICZ.

## II. Western Michigan University Theft

9. I have reviewed WMU Police Department (WMU PD) incident report 2026-8832, and am aware that on June 23, 2026, a WMU employee contacted police to report *"Red, Blue, Yellow"* was missing from its storage location in WMU's Richmond Center. WMU PD conducted a review of surveillance video footage in the area and noted a white male wearing glasses, a grey with horizontal striped tee shirt and grey jeans carrying a backpack and walking throughout the building around 9:46

AM that morning. At 9:56 AM, the subject was observed carrying *"Red, Blue, Yellow"* out of the area where it was being displayed.

10. I reviewed a portion of the video surveillance footage of this incident and observed the subject responsible for the theft was carrying a cellular device in his hand immediately prior to the theft.

11. Through further review of surveillance video footage, WMU PD determined the subject arrived at WMU's campus in a white Lexus ES300 (the Subject Vehicle) which parked in the area near WMU Lot 35 around 9:43 AM. The subject entered an elevator near Lot 35 at 9:46 AM. At 9:59 AM, the same white Lexus ES300 could be seen departing the area. WMU PD observed through surveillance video the digits "777" in the Michigan license plate of the white Lexus. Utilizing license plate reader records, the full license plate of the vehicle was determined to be ENX7771. WMU PD conducted an inquiry with the Michigan Secretary of State and determined the registered owner of the Subject Vehicle was W.S.[1] of Ada, Michigan.

12. WMU PD utilized a still image from the surveillance video and submitted it to the Michigan State Police for facial recognition analysis. The Michigan State Police provided an investigative lead based on this query that the subject involved in the theft was probably MIKOLAI STASIULEWICZ (hereinafter referred to as MIKOLAI.)

[1] The identity of this individual is known to me, however, I am choosing to conceal their identity for the purposes of maintaining their privacy.

## III. Muskegon Museum of Art - Subject Spotting

13. In speaking with WMU PD, I learned they had been contacted by the Muskegon Police Department (MPD), who told them a subject matching MIKOLAI's description had also stolen art from a museum in their jurisdiction.

14. I have reviewed MPD incident report MU2610025, and learned that on June 25, 2026, a subject matching MIKOLAI's description visited the Muskegon Museum of Art (MMOA). The subject appeared to be "casing" the area, and entered several "employee only" areas of the museum during his visit. The subject was inside MMOA from about 5:30 PM to 6:16 PM.

15. MPD conducted a search of license plate reader records and observed the Subject Vehicle was spotted within 2 blocks of MMOA at 5:23 PM. I reviewed surveillance video footage from MPD and observed that the subject appeared to be wearing the same striped t-shirt and shoes MIKOLAI was wearing during the WMU theft on June 23, 2026. I also observed he was carrying a "TJ Maxx" shopping bag on his shoulder during his visit to MMOA.

16. While reviewing the video surveillance from MMOA, I noted MIKOLAI was holding a cellular device in his hand.

## IV. Grand Rapids Art Museum Theft

17. I have reviewed reports from Grand Rapids Police Department (GRPD) incident no. 26-046167. I learned that the GRAM contacted GRPD on July 2, 2026, to report the theft of *"The Sudarium Held by One Angel*" from its collection. GRAM staff advised GRPD a white male wearing a blue shirt, tan shorts and a black hat took a

painting off the wall and left the building. The GRAM also reported the same subject was at the museum on June 17, 2026, in what appeared to be a pre-theft surveillance visit.

18. GRPD obtained and reviewed surveillance video from the theft on July 2, 2026, and found the male subject identified by the GRAM matched MIKOLAI's appearance. I have reviewed portions of this surveillance video and observed MIKOLAI was holding a cellular device in his hand around 5:10 PM, just before the theft of the art work.

19. On July 20, 2026, GRPD Detective Juan Escamilla interviewed W.S., the registered owner of the Subject Vehicle. W.S. told Det. Escamilla that he/she was an immediate family member of MIKOLAI, and had sold him the car about three months earlier. Later that evening, W.S. contacted MIKOLAI by phone to confront him about the police investigation. W.S. called Det. Escamilla and advised that they had called MIKOLAI at (616) 930-1640. W.S. further advised that they believed MIKOLAI was staying at 147 Burr Oak St Northeast, Grand Rapids (hereafter 147 Burr Oak). GRPD was unable to immediately locate MIKOLAI at that address.

20. On July 30, 2026, Det. Escamilla advised me that GRPD patrol officers were dispatched to 147 Burr Oak, where they found MIKOLAI STASIULEWICZ deceased of a suspected drug overdose. Officers recovered the Devices from the bedroom as part of the death investigation and logged them into GRPD's secure evidence facility.

21. On July 31, 2026, FBI and GRPD conducted a search of 147 Burr Oak St Northeast, Grand Rapids, Michigan with the consent of the owner and MIKOLAI's roommate. Four pieces of artwork, including *"Red, Blue, Yellow"* and "*The Sudarium Held by One Angel"* were recovered from MIKOLAI's bedroom at the residence.

## V. Additional Details

22. Through service of legal process, I am aware MIKOLAI met with an individual identified as John Supanich, at the Gun Lake Casino, located at 1123 129th Avenue, Wayland, Michigan, on the evening of July 8, 2026. The purpose of the meeting is unknown, however, video surveillance records indicate MIKOLAI departed Supanich's hotel room holding an unknown amount of cash in his hand and departed from Gun Lake Casino shortly after.

23. As part of this investigation, a query was made of open source records regarding MIKOLAI. Several articles were found describing MIKOLAI as an amateur artist who studied at the Interlochen Center of Arts in Interlochen, Michigan.

24. In my training and experience, and that of the Art Crime Team, phones and computers like the Devices will often be used to communicate with co-conspirators. Specifically, they may contain evidence of communications about what art pieces to steal, negotiations for sale prices, and arrangements to transfer and "fence" the stolen works. They are also typically used to store contact information for associates, calendar entries regarding meetings, and other information from which the identity of co-conspirators can be determined. They may also include search history information relevant to the scheme, and electronic traces of contacts with sites

like dark web forums for the sale of stolen property. In addition, most people carry their cellular telephones with them when traveling outside the home. Because phones keep records of their past GPS coordinates, the Devices may show where MIKOLAI traveled to meet with co-conspirators, buyers, and/or facilitators of prospective sales.

## DEFINITIONS AND TECHNICAL TERMS

25. Based on my training and experience, I used the following technical terms to convey the following meanings:

26. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communication, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

27. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

28. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

29. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address

so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

30. Based on my training, experience, and research, I know that the Subject Devices have capabilities that allow them to serve as a wireless telephone, digital camera, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time, including years. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. Even if an individual is being cautious of law enforcement detection and deleting files related to the Subject Offenses, significant data may remain on the phone, such as call logs, contact information, photographs, wireless internet connections (which can reveal location information), and other location information.

32. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of

the use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Devices because:

33. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

34. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

35. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

36. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

37. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

39. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

40. Based on the above information, I respectfully submit there is probable cause to believe that there will be evidence of the Subject Offenses on the Subject Devices, and request that the Court issue a Search Warrant authorizing the search of the Subject Devices, described in Attachment A, for items listed in Attachment B.