IN THE CIRCUIT COURT OF THE STATE OF OREGON

FOR THE COUNTY OF DESCHUTES

2022 SEP -1 PM 4:52

STATE OF OREGON		AFFIDAVIT FOR
COUNTY OF DESCHUTES	SS	SEARCH WARRANT
		22AD03256

I, Detective Eli Allen, first duly sworn on oath, hereby depose and say:

This affidavit establishes probable cause to believe, and I do believe that the crime(s) of Murder, ORS 163.115 and Murder, ORS 163.115, has/have been committed and are triable in Deschutes County, Oregon, and that evidence of these crime(s) will be found at the locations listed herein.

I. Training and Experience

I am a sworn police officer employed by the Bend Police Department as described in ORS 133.525(2)(b) and I am aware that ORS 133.535 (2) specifically authorizes the search and seizure of the fruits of the crime, and that ORS 133.535 (3) specifically authorizes the search and seizure of the property that has been used or is possessed for the purpose of being used to commit an offense. I am aware that these sections specifically authorize the search and seizure of the above described items pursuant to a criminal search warrant.

I have over 5 years of experience in investigations and am currently assigned to the Investigations Division as a Criminal Detective. I have been a police officer with the City of Bend Police Department since September 2019, and a detective since July 2022. Prior to employment with the City of Bend, I was Deputy Sheriff with the Washington County Sheriff's Office from July 2017 to September 2019. I have Bachelor's Degree from the University of Kansas and a Juris Doctorate from Washburn University School of Law. Currently, I possess an Intermediate Public Safety Officer certification from Oregon Department of Public Safety Standards and Training. I have received over 1243 hours of documented law enforcement training in many aspects of police work to include but not limited to: interview and interrogation techniques, various case law, evidence collection and preservation, search warrants and criminal investigations. This training has been provided by Oregon Department of Public Safety Standards and Training, Bend Police Department in-service trainings and from other various agency's within the State of Oregon.

Furthermore, I have conducted and/or participated in investigations of all types of crimes including but not limited to sex crimes, child abuse (both sexual and physical), weapons offenses, assaults, domestic assaults, kidnapping, robbery, menacing, traffic crimes, burglary, theft, fraud, unlawful use of a motor vehicle, arson, computer related crimes, internet investigations and drug enforcement. This experience has also included locating, photographing, collecting and processing evidence associated with those types of crimes.

I have attended 8 hours of unique training specifically related to online luring and child sexual abuse. I have interviewed victims of sex crimes and suspects while conducting investigations. Within this

experience, I have talked to suspects about their mindset, methods, desires, fears, and purpose for committing these crimes.

Since my employment with Bend Police Department, I have used, and continue to use on a daily basis, several computer databases for investigative purposes. I have found these computerized data bases, including but not limited to the Law Enforcement Data System (LEDS), the National Crime Information Center (NCIC), the Deschutes County computerized files, (COPS), AEGIS, LERMS, Deschutes County DIAL, and the Deschutes County 911 dispatch files, to be accurate and reliable sources of information. On hundreds of occasions I have retrieved information from one or more of these databases and then later confirmed the validity of the information by further investigative techniques.

II. Summary of Affidavit

There is probable cause to believe, and I do believe, that the evidence described below will show that Ethan Blair Miller (DOB 10/31/2001) engaged in the crimes of: 8/29/22

Murder, ORS 163.115 and Murder, ORS 163.115.

III. Application for Search Warrant

Application is hereby made for a search warrant to search the following:

Apartment number . located in the Fox Hollow Apartments. The complex is located at 2600 NE Forum Dr., Bend, Deschutes County, Oregon. Apartment number is located on the 1st floor of the building marked with the letter/number The building marked with the letter/number is gray in color with gray trim and a composite roof.

A Blue 1997 Ford F-250 bearing Oregon license plate . This vehicle is registered to Ethan Miller and is currently located at 2600 NE Forum Dr., Bend, OR 97701.This vehicle was under the control of or accessible to Ethan Blair Miller (DOB 10/31/2001).

IV. Item to be Searched for and Seized

Application is hereby made for authorization to photograph, search for, seize and analyze the following evidence:

Digital devices capable of storing user data (i.e. cellular telephones, computers, tablets, GPS units, removable storage) which were in the possession of and/or accessible to Ethan Blair Miller (DOB 10/31/2001).

Blood, biological fluids, hairs, fibers, and DNA evidence found in the location(s) outlined in this search warrant.

A forensic firearms analysis to include a general firearms exam, an exam of the operability and exam of the ammunition including an ammunition count.

Ballistics evidence and analysis of the firearm and of spent casings as well as unexpended cartridges.

Firearm trajectory evidence found in the location(s) outlined in this search warrant.

All firearms in the possession or control of Ethan Blair Miller (DOB 10/31/2001). DO 8/29/22

Firearm ammunition, used/spent shell casings, bullet fragments, and/or bullet jackets, as well as Molotov cocktails or bomb-making devices or materials.

Firearm accessories to include; firearm magazines, ammunition storage devices, feeding devices designed to be attached to a firearm, cleaning supplies, cases, manuals, sights, grips, reloading accessories, holsters, and/or optics.

Verified Correct Copy of Original 9/8/2022

V. Local Investigation

On 8/28/2022, I responded to a reported active shooter occurring at the Safeway Grocery Store, located at 2650 NE Hwy 20, Bend, Deschutes County, Oregon 97701. After I arrived, I learned that a single male suspect had entered the grocery store armed with what appeared to be an assault style rifle, and a black pump shotgun. Officers who entered the store confirmed and relayed to me that after firing both weapons inside and killing two people inside the store, the suspect took his own life. While at the scene, I was directed to interview told me that his friend, Ethan Miller DOB (10/31/2001) had texted him earlier in the evening and made suicidal comments. After receiving these text messages, drove the Miller's home, located at 2600 NE Forum Dr., Unit Bend, Deschutes County, Oregon 97701. intended to check on Miller, but found many police vehicle responding to the area due the report of an active shooter.

told me Miller owns a black 5.56 caliber AR15 style assault rifle and a black 12-gauge pump shotgun. told me that Miller lives at the Fox Hollow Apartments, located at 2600 NE Forum Dr., Unit , Bend, OR 97701. also advised Miller lived at this apartment with his brother, and his mother, also advised me that Miller drives an older model Ford F-250 pickup truck, which was parked in front of apartment

Bend Detective Sergeant Eric Hagan showed me a photograph of a deceased male located inside of Safeway. I have known Sgt. Hagan for approximately 3 years and know him to be an honest and trustworthy person. The male appeared to be a white, male adult, approximately 18-25 years old. The male was wearing all black and had a pump shotgun lying next to him. Sgt Hagan showed me another photograph of an AR15 assault style rifle laying on the ground inside the Safeway. This deceased male was believed to be the suspect.

At this time, I advised Sgt. Hagan and Bend Lieutenant Adam Juhnke of what I have learned from I located a Facebook page for a male named 'Ethan Miller'. The account stated that this male was from Medford, OR but was currently living in Bend, OR. One of the photographs from the account is two white, male adults approximately 18-25 years old, holding what appear to be an AR15 style assault rifle and a black pump shotgun. I reviewed this photograph with Lt. Juhnke and compared it to the photograph of the deceased male inside Safeway who was believed to be the suspect. The deceased male appeared to be the male on the left of the photograph who is holding the AR15 style rifle.

After learning this information, I believed Ethan Miller was the suspect. I then partnered with Redmond Police Officer Michael Maloney, and we went to Fox Hollow Apartment my unmarked vehicle. Outside of the apartment, I observed a group of approximately 5 to 10 individuals standing directly outside of unit , along with many other persons walking through the complex. I observed unit is located in Building . It is a lower level unit in an eight-unit building. The unit is the unit from the south. The front door faces to the west. The building is gray in color and the front door is a darker color gray. The numbers are posted to the south of the front door.

Parked approximately 3 spaces to the north of the front door of unit , is a blue two-tone 1997 Ford F-250 pickup stuck bearing Oregon Plate . The vehicles Oregon Department of Motor Vehicles return lists the registered owner as Ethan Miller The vehicle has a broken rear windshield. In the rear passenger seat there is a box of 5.56 Winchester ammunition and box of 12-gauge shotgun shells.

While sitting at outside the apartment, I was advised by Bend Police Detective Rob Pennock that , Miller's mother, had stated to him that Miller owned two firearms, an AR15 style assault rifle and a 12-gauge shotgun. I have known Det. Pennock for three years and know him to be an honest and trustworthy person. Det Pennock also told me that said Miller keeps both firearms under his bed in the residence.

While still at the apartment, I was advised by Deschutes County 9-1-1 that they were receiving multiple calls regarding social media posts Miller had made across several platforms including saying that when the post was read by others he would be dead and that he had Molotov cocktails. Molotov cocktails are a kind of improvised explosive device or bomb. These statements were confirmed to me by Detective Russ Skelton who had viewed them. Bend Detective Russell Skelton advised that efforts were being made to preserve these posts.

A male who lives in unit directly above unit , showed me video taken from a camera that points down the stairwell onto the sidewalk area in front of unit The video shows what appears to be a male leaving unit dressed all in black. The male is carrying what appears to be a rifle. As the male steps onto the sidewalk, he raises the rifle and fires to the north. After shooting at least one time, the

male then begins to walk south and out of the frame of the camera. I believe this male was Miller leaving is apartment and firing into his 1997 Ford Pickup.

As I write this affidavit, it is after 11:00 p.m. on August 28, 2022. I believe that evidence may be moved or may dissipate if service of the accompanying search warrant is delayed. I therefore request nighttime service of the warrant be allowed.

VI. Basis of Knowledge

Person Crimes

Based on my training and experience, I know that persons involved in violent physical crimes, do so for a wide variety of reasons to include, but not limited to: revenge, personal satisfaction, anger, emotional outrage, financial gain, concealment of other crimes, and sometimes as the result of intoxication, substance abuse, and/or mental crisis. The motives of the suspect(s) may be found documented in areas such as, but not limited to: journals, notes, digital devices, financial documents, marital records, medical and/or mental health records.

Assaults

From my training and experience I know that many objects can be made or altered into a weapon that can cause serious physical injury or death even if the object is not specifically designed to cause serious physical injury and/or death. I also know that many weapons, when used against another person, are designed for the purpose of causing serious injuries or death (i.e. knives and firearms).

Conceal/Destroy Evidence

I know from my training and experience investigating numerous violent crimes, that persons attempt to conceal, discard, and/or destroy items used when planning a crime. They will often attempt to conceal these items in the residence of the person, near their residence, in a vehicle accessible to the person, near their place of employment, near the crime scene or other familiar locations to the suspect. I know that in cases where the suspect(s) conceals, discards, and/or destroys items that have evidentiary value to the investigation in places that are not familiar to the suspect, they likely accomplish this between the location of the crime and the residence of that person. These locations including, but are not limited to: the bathroom (toilet) used by the person, garbage cans, closets, inside dressers, under mattresses in their beds, in locked boxes and safes in their living space, storage outbuildings, vehicles, and any other location where they could be easily and conveniently concealed.

Trace Evidence

I know from my training and experience that persons involved in the planning of violent crimes often attempt to conceal evidence by destruction, discarding, laundering, or burning items which contain

trace evidence, or might otherwise serve to identify them as the perpetrator. I know from my training and experience that evidence is often transferred to other surfaces (i.e. bedding, carpet, flooring, walls and clothing), I know from my training and experience that even when clothing, bedding, or other material is laundered and/or cleaned, a trained crime scene technician skilled in the retrieval of evidence can still collect evidence that may not be readily visible to the naked eye.

Intentionally Planning for Crime

Persons who commit these crimes often spend days, weeks or months prior to the crime planning, thinking, dreaming, researching, or trying to discover ways to better carry out the crime. These steps may be documented or stored in handwritten journals, notebooks, ledgers, photographs, audio and video recordings, computer files, and other electronic data storage. It is common for individuals to make diagrams, maps, and written communication outlining their plan. Those diagrams, maps and written communications, if not destroyed can be located within a vehicle, residence, or the digital devices of the suspect. I also know from my training and experience that people who commit these crimes will often display interest in the crimes and others who have/are committing them. I know from my training and experience that people who commit these types of crimes will research the crimes by reading books, articles, blogs, forums, and performing Internet-based research on the crimes and related topics. I know related research may be for the preplanning of the event and often takes place weeks, months or even years prior to the commission of the crime(s). I also know from my training and experience that people express interest in these types of crimes by researching people who have previously committed these crimes or on the best methodologies for the commission of these crimes. This would include methods for destroying evidence, disposing of evidence, and evading law enforcement capture. I know that even after the crime is committed suspects will often research information about the crime, research how to conceal evidence, research potential consequences, communicate with others about the crime, attempt to establish an alibi, or keep current on the investigation.

I also know from my training and experience that persons who commit these crimes will likely exhibit changes in behavior and demeanor before, during, and after the commission of the of crimes. The changes in behavior are likely to become evident in their communication with friends, families, coconspirators, and victims in the days, weeks, and months leading up to, or following, their crimes. I know that currently the most prevalent way to accomplish the above-mentioned actions is through the use of digital devices (i.e. cellular telephones, computers, tablets).

Based on my training and experience, I know that persons committing violent crimes do so for a wide variety of reasons to include, but not limited to: revenge, personal satisfaction, emotional outrage, as the result of intoxication and/or substance abuse.

Casing Target

I know from training and experience that persons committing crimes will often case an area to observe preselected targets or to identify new targets. This observation period is when the suspect(s) will gather intelligence about their target such as; surveillance systems, methods of entry, possible items to take, and required tools. During this part of the intelligence gathering process suspect(s) may document their target with notes, pictures, or with digital searches of the area. It is also common for these suspect(s) to make contact with people in the area whether they are concerned about the suspect(s) behavior or trying to be helpful.

Search Vehicle

I know from my training and experience that persons who commit crimes likely use a vehicle to facilitate the preparation or commission of the crime. When travelling to the location a vehicle is often used because it allows for the transport of tools/supplies A vehicle is also likely to contain documents and other physical items of information regarding the location of the crime, suspects movements, and/or preplanning of the crime. A vehicle also gives suspects the ability to transport proceeds of the crime (i.e. stolen items) and make a speedy getaway from the area the crime was committed. A vehicle will also likely contain trace evidence from the scene (i.e. broken glass).

Digital Components - Property Crime

Based on my training and experience, I know that persons who commit violent crimes will often use computers and the Internet to research, communicate about the crime, and keep notes. Persons who commit crimes also use digital devices to keep receipts, stock portfolios, bank records (showing debits and credits), transfer funds, and keep diaries and journals where they record their offenses, names of their victims, financial gains, and keep track of their activities. The above listed items can be kept in many forms including, but not limited to, written, typed, or various types of computer files.

Weapons Offenses

I know from training and experience that persons often commit weapons offenses for reasons such as intoxication, anger, robbery, intimidation, emotional outrage, and revenge. I also know that when a person is in possession of a firearm and/or other weapons during the commission of the crime, additional firearms and or/weapons are often stored/kept at the person's residence, outbuildings, and/or property for long periods of time.

Firearms

I know from my training and experience that firearms and/or weapon's accessories including, but not limited to: the weapons themselves, ammunition, shell casings, bullets, magazines, cleaning equipment, holsters, gun boxes and cases, trigger locks, gun safes, gun parts and tools, targets, receipts, and bills of sale are all relevant to the possession, dominion, and control of a weapon. I know from my training and experience that when a firearm and/or other weapon is utilized in the commission of a crime many times victims and/or witnesses can describe the item to include size, make, model, or color. I also know that it is possible through forensic testing of firearms and/or other weapons to locate trace evidence that relates to the person who utilized the weapon.

I know from training and experience that people who possess firearms will often have other items associated with firearms. I know that these items often include cases, ammunition, holsters and documents indicating ownership. I know that it is common for people who possess firearms to have additional firearms. I know that firearms and ammunition can commonly be carried in very small containers.

Concealed/Hidden Weapons

Further, I know based on my training and experience that persons who commit weapons offenses, including those who are prohibited from possessing certain weapons, will attempt to conceal those weapons. They will attempt to conceal those weapons in locations, including but not limited to, vehicles, personal property, and environmental concealment (i.e. under rocks, in trees, behind natural barriers,

etc.). I know, from my training and experience, that people who possess weapons will often inadvertently document their possession of the weapons through photographs, videos, and personal correspondence. Concealing of firearms, is a practice of persons in the criminal community, and is an attempt on their part to prevent the firearms from being stolen by other persons, and to prevent their firearm and firearm accessories from being discovered by law enforcement in the event of the service of a search warrant.

Firearm Trace Evidence

I know from training and experience that when most firearms are discharged, shell casings can be ejected onto the ground. I also know that when people possess firearms that a person normally will also possess corresponding ammunition for related firearms within their residence. I also know that bullet(s), bullet fragments and bullet jackets can be collected and scientifically compared to firearms, to determine if the bullet(s), bullet fragments, shell casings, and bullet jacketing were fired from a particular firearm.

I know through training and experience that suspects and the surrounding environment will often accrue trace evidence from the act of shooting firearms. I also know that other trace evidence is expelled out of a firearm with a bullet which can sometimes be transferred to a victim, wall, or other surfaces.

I also know through training and experience when guns are fired, evidence in the form of bullet holes, bullets, bullet fragments, and shell casings from weapons fired, may be located in surrounding structures, vehicles, vegetation and/or clothing. Analysis can be conducted with the utilization of specialized equipment that will aid in determining positions of those who fired a weapon and the trajectory of their fire. Furthermore, I know that some evidence can only be obtained by removing or cutting the evidence from surrounding area including, but not limited to, bullet holes in surrounding drywall and blood or other bodily fluids in carpet or other materials.

Trading/Selling Weapons

I know from training and experience that persons involved in the commission of weapons offenses will often attempt to obtain cash, valuables, and/or other weapons that they can use to commit further crimes or as currency in their escape / travels. I further know that persons responsible for committing weapons offenses will often times keep items taken for an extended period of time until they feel it is safe to use items in ways including, but not limited to: trade, consignment, or pawning, such items, or in some cases, keep such items indefinitely with no immediate intention of transferring such property to another.

Physical Forensic Evidence

I know based on my training and experience that the Oregon State Police (OSP) Forensic Services Division is accredited by the ANSI National Accreditation Board (ANAB). They are certified every four years by ANAB and every year ANAB conducts surveillance assessments to insure quality control. The OSP Crime Lab can conduct scientific analysis of the following: firearms, clothing, fibers, hair, body fluids, fingerprints, controlled substances, DNA, trajectories, bloodstain patterns and other trace evidence.

Test Firearms / Ballistics

I know from training and experience that technicians with the Oregon State Police Crime Lab are

training in the examining of firearms. I know that these technicians are capable of examining the operability of a firearm. I know that they are capable of examining the ballistics of rounds fired and can attempt to re-produce any malfunctions that may have happened in the past. I know that they can examine the expended, intact and damaged rounds to better determine the cause of malfunctions as well as determine the probability that a round was fired

Use of a Drone

I know the Deschutes County Sheriff's Office, Oregon State Police, Redmond Police Department, and the Bend Police Department own and operate Unmanned Aircraft Systems as defined in ORS 837.300(1). I know these Unmanned Aircraft System are registered with and comply with all Oregon Department of Aviation and Federal Aviation Administration (FAA) laws and regulations. I know these agencies employ pilots trained to operate the Unmanned Aircraft Systems within all local, state and federal regulations.

I know the Unmanned Aircraft Systems collect and record visual media evidence in the form of digital photographs and digital video. I know the camera on the Unmanned Aircraft System is capable of capturing images both during the day and at night using high definition lenses and thermal technology.

I know through training and commutation with the above-mentioned pilots that Unmanned Aircraft Systems are typically utilized when serving a search warrant in two ways; surveillance and documentation of a scene. I know that when using an Unmanned Aircraft System for surveillance it is more discrete and creates less risk to law enforcement officers than other means such as direct surveillance. I also know that when using an Unmanned Aircraft System for surveillance it is less intrusive than other means such as direct surveillance. I also know through my training and experience that when utilizing an Unmanned Aircraft System for the collection of images and digital video, specifically for the purpose of documenting a scene, it is one of the only ways to provide overall documentation. This overall documentation provides powerful context for viewers who have never been to the scene of a crime.

I know ORS 837.320 (1) (a) allows for the operation of an Unmanned Aircraft System by a law enforcement agency to acquire and disclose information upon the issuance of a warrant.

Digital Evidence

I know from my training and experience that digital devices have the ability of storing, processing, and/or outputting digital data. There are a wide variety of digital devices where digital data can be interacted with in this way. This includes but is not limited to: cellular phones, desktop, laptop, and tablet computers, servers, video game consoles, computer hard drives in various forms such as platter drives and solid state drives, compacts discs (CD), digital versatile discs (DVD), thumb drives, flash drives, media cards, iPods/mp3 players, any other form of optical, flash, or magnetic storage which is capable of being used as a repository of data, and networking equipment such as routers and modems. In addition to digital devices, digital services allow for a streamlined experience with digital data between different digital devices used by a single person as well as between different persons of different digital devices. There are a wide variety of digital services where digital data can be interacted with and shared in this way. This includes but is not limited to: data synchronization and cloud based data services offered by major manufactures such as Apple, Google, and Microsoft, social media platforms such as Facebook, Twitter, LinkedIn, and Instagram, peer to peer services, and streaming services such as YouTube, Netflix, and Hulu.

I know that by the most conservative of estimates, the majority of adults in the United States of America own or use digital devices and services; over 80% own cellular telephones, over 70% own specifically smartphones, over 70% own computers, over 80% actively use the Internet, over 60% use some type of Social Media, and over 50% use some sort of streaming services. Digital devices and services are a daily aspect of American's lives, and knowledge of the use of digital devices and services are a requirement and necessity through grade school and higher education.

Digital devices, services, and data are in a continuous state of evolution and refinement. Persons use digital devices every day for activities such as communication, text messaging, emailing, browsing social media, productivity, entertainment, taking pictures, data storage, data retrieval, calendaring, and surfing the Internet. In the process of normal operation, digital devices create, store, retrieve, alter, and process digital data related to the user of the device, including their work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations. This is common across all persons using digital devices, including those whose work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, or associations are criminal in nature. Digital devices contain information automatically created by operating systems, software, and applications, which the user of the device is more often than not unaware of. This information includes data regarding user interaction with a device, backups and data synchronization, cloud-based data and interaction, hidden, encrypted, and password protected information, as well as locational information.

I know that digital devices can access, create, modify and store communication data. Communication data includes any type of data designed or capable of being used for communication. This data may include text, audio, and multimedia communication, as well as information about who is participating in the communication. Communication can be effectuated by SMS/MMS, chat messages, social media, voicemail, email, as well as any other means of digitally communicating between digital devices I know that most people use digital devices to communicate with others on a regular basis including with friends, family, coworkers, acquaintances, and other persons. This is true also with persons involved in criminal activity, where that communication includes being with co-conspirators, victims, and witnesses. I know that when a digital device is used for communication, data is created on the device, and this data may indicate information such as dates and time of communication, communication content, user names, email addresses, IP addresses, and other types of data. This data is often valuable evidentiary information in criminal investigations. For example, a suspect might discuss a crime over text message, or a suspect might leave a voicemail apologizing to a victim for committing a crime.

I know that many digital devices allow users to create, access, and/or store digital image, audio, video and multimedia files. I also know that many digital devices contain operating systems, applications and software that do the same. People document activities and events in their daily lives using digital devices, such as recording conversations or voice memos, or taking pictures or videos of birthdays, vacations, family and friends, or other hobbies, interest, and memorializations. These documented activities and events are often download, copied, and duplicated to and from other digital sources and devices for later retrieval and long-term storage. They are also shared, copied, and duplicated digitally amongst friends, family, coworkers, acquaintances, and other persons by means of messaging, emailing, posting to social media, etc. This is true also with persons involved in criminal activity, where persons document criminal activities by photographs, videos, as well as digital memos, texts and audio recordings. Persons involved in criminal activity also share, copy, and duplicate these files the same amongst co-conspirators, victims, and witnesses. This data is often valuable evidentiary information in criminal investigations. For example, a suspect might record a video documenting a crime as a memorialization to reflect on later or share with other persons, or a suspect might take an image of illegal items as proof to share amongst others who share in the same work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations.

Verified Correct Copy of Original 9/8/2022

I know that many digital devices can access, create, modify and store many different types of documents. Documents encompass all manner of files including electronic documents containing text, numbers, and special symbols which are typically used for human readable communication, storage of information, and presentation. While a large variety of documents exist, common document files include, but are not limited to, Microsoft Word, Excel, and PowerPoint files, pdf files, text files, notes, journals, word processing documents, and spreadsheets. People use documents for a vast assortment of reasons; to memorialize dates, activities, and events, to communicate important information, to maintain a record of information for later reference or work purposes, to pay bills and keep financial records, to understand how products and items work through digital user manuals, to compile comparisons of data, etc. Persons can create documents which may be personalized, and operating systems, applications and software can create documents to record specific activities. This is true also with persons involved in criminal activity, where the documents contain the same types of information which are criminal in nature. This information can be very valuable to criminal investigations. For example, a suspect might document dates and times while casing locations for future criminal activity, or keep ledgers and transactional records of their criminal activity. Such personalized documents can provide further valuable insight temporally, for example if a contraband file was accessed in close temporal proximity to a modification of a personalized document, the temporal proximity is indicative of the contraband file being accessed by the same user who modified the personalized document.

I know that many digital devices can access the Internet and in the process create and store digital information related to Internet activity. I know users can access Internet resources through browsers and software clients. While accessing the internet, digital devices store a large amount of information detailing what the person was using the internet for, including user searches, browser history, cached data, form data, social media data, and blog posts. People use the internet to search for and view websites, access and share multimedia files and documents, communicate with other persons via social media and blogs, research information, and buy, sell, and trade items, among a number of other reasons. For most people, the internet is a common part of everyday life and activity regarding their work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations. This is true also with persons involved in criminal activity, where their use of the internet is the same but for purposes that are criminal in nature. This information can be valuable to criminal investigations, as it can reveal motive, planning, knowledge, a transfer of ill-gotten gains, concealment attempts, and/or attempts to discover detection by or evade law enforcement. It can also reveal methods and means of research, networking, and collaboration of criminal activity. For example, a suspect might research the resell cost of goods which were obtained or are possessed illegally, or search and research websites where persons who share the same work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations which are criminal in nature, can share their ideas, methods, and material.

I know that through the normal use of a digital device, the operating system, software, and applications all create data which is not easily accessed by the user. This data details how the user is interacting with the device and with different software and applications This data could be used by the respective platform which is creating the data in order to show the user their usage history, make suggestions based upon their previous usage, or as usage statistics for the creator of the platform to troubleshoot or continue expanding and upgrading their product and services. This is in line with manufactures and service providers consistently striving to streamline data and the experience of their users, and is enveloped in the persons use of their device regardless of their work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations. This information is highly customized and unique to how a particular person is using a device. This is true also for persons involved in criminal activity, where the user's interaction of a digital device surrounds work, activities, hobbies,

interests, likes and dislikes, memorializations, achievements, and associations which is criminal in nature. This information can be valuable to criminal investigations, as it can reveal indications of ownership, use, and/or dominion of control over the device to show the identity of the person at the time and place any evidentiary information is located It can also show a person's pattern and behavior in regards to events leading to, during, and after the criminal activity is committed. For example, user interaction logged by mapping applications would show a person searching for directions to and from an address of a residence which would become the target of their next burglary, or user interaction of an operating system would show a user accessing their camera application and turning on a video recorder for their camera prior to a crime being committed and turning the recorder off after the crime was committed, even if the video was unable to be found.

I know persons keep digital data for long periods of time, backup copies of important data to other digital devices, and transfer data between devices which creates copies of data between the devices, both knowingly or unknowingly. This process is done manually by the user of the digital device for data which they deem important, such as conversations, images/videos, website bookmarks, emails, and applications themselves among other forms of data This data is important to the user in some way regarding their work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations, and can be for various reasons from preserving a memory or interest, to providing and keeping documentation for future reference. People backup data from their digital devices to all sorts of digital storage media, including to the digital device itself through another storage method, external hard drives, USB and Flash drives, storage media cards such as SD and microSD cards, computers, cellular telephones, and CDs and DVDs. A person may also create a backup of an entire digital device to serve as a fallback in the event a device is lost, broken, or a new device is purchased. Backup functions are available as a standard by major device manufactures, such as Apple, Google, and Microsoft. This is true also for persons involved in criminal activity, where the data backed up surrounds work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations which is criminal in nature. This information can be valuable to criminal investigations, as it can show the transferring and obfuscating of criminal activity and show the attempts to separate criminal and noncriminal interaction with digital devices. For example, a suspect may use a device to download child exploitation material, and move that material to a different storage device in order to give the appearance that no criminal activity is occurring on the original device, or a suspect may take a screenshot of a conversation about the purchasing and sales of illegal items in order to provide proof of an agreed upon deal. Aside from data being manually backed up by a person, this can also be done automatically, without any particular input from the user, through data synchronization between digital devices.

Data synchronization is the process of establishing a consistency of data between digital devices, ensuring that the same data or version of data exists across all devices where the synchronization is taking place. The process of data synchronization has been adopted by and is a standard of major digital device manufacturers and service providers, such as Apple, Google, and Microsoft. Each manufacturer and provider has their own specific method of accomplishing data synchronization with the general idea and end result being similar, data from one device is synced between other devices accessed by the same user in order to provide streamlined productivity, a more seamless user experience, and provide access to data and backups of devices in the event of a loss, failure, or new device. Although the methods are different, the data synchronization is not isolated within only digital devices and services offered by one entity. For example, a person with a device from Apple, such as an iPhone, can achieve data synchronization between other Apple devices, Android (created by Google) based phones, and Windows (created by Microsoft) based computers. This allows the user to access photos, videos, messages, notes, calendar entries, email, and other data which were originally created or accessed on the single device across all other devices for which the user had access and logged

into. The general idea and concept of data synchronization is similar amongst Android (Google) devices and Windows (Microsoft) devices as well. When using these devices for the first time, data synchronization is turned on by default for accounts created with digital devices connected to the internet from these manufactures and service providers. This is true also for devices used by persons involved in criminal activity, where the data being synchronized by default across devices is criminal in nature. For example, a suspect may have multiple phones and computers which they have activated with their Google account. Though they may have destroyed or otherwise deleted and removed data from one device, that data will more likely than not have been shared through data synchronization to the other devices which may not have been known to the investigator previously.

Aside from data synchronization, each of these major device manufacturers and service providers also provide cloud based storage of data by default for free with certain size limitations; Apple iCloud at 5 Gigabytes, Google Drive at 15 Gigabytes, and Microsoft OneDrive at 5 Gigabytes. Every account created through these providers comes with the default free cloud storage, and also allows for paid subscriptions to increase the storage amounts. As opposed to data synchronization where the data originally exists on a specific digital device and is consistent across other digital devices, this cloud storage allows access from anywhere and everywhere with digital devices, while still maintaining the core of the data within the cloud service. This allows for interaction with the data contained within the cloud service, without having to synchronize the same data between devices. Examples of this would be maintaining documents within the cloud service that could be opened, edited, and modified from any digital device, or maintaining other forms of data within the cloud service to serve as a type of backup that is accessible anywhere at any point in time. There are several other cloud storage providers, including DropBox and Amazon Drive, that offer this same type of service for free while requiring you to create a different account other than the account you created originally for the digital device itself. This is true also for persons involved in criminal activity, where the data they wish to access from any digital device at any point in time is criminal in nature. For example, a suspect may keep a ledger on their Google Drive account of transactions of illegal items in order to access the ledger from any device in an attempt to keep the illegal information off of their device, or in the event they lose or damage their original device.

I know from my training and experience that privacy is at the core of marketing for major device manufacturers and service providers, including Apple, Google, and Microsoft. Whether hiding, password protecting, encoding, or encrypting data, the interest of privacy is a default functionality for most digital devices today, as well as the data that the digital devices handle and transmit electronically. Password protecting devices is a default standard option when setting up most digital devices for the first time, and most digital devices provide functionality which is easy to access and use in order to hide and encrypt specific data on those devices. Beyond the standards set forth by major device manufacturers and service providers by default, third party applications and service providers such as Facebook Messenger, Snapchat, and various Secret Calculator providers, offer simple means to password protect, hide, or otherwise encrypt data as directed by the user. These applications and services are easy to access and use, and generally are free to the user. Persons can hide, password protect, or encrypt individual files, contents of an entire folder, or the totality of a digital storage media quickly, easily, and without the need for a deep or technical understanding of technology This is used by persons who maintain sensitive information, including documents, conversations, and photos, videos, and recordings, relating to their work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations. This is true also for persons involved in criminal activity, where the data being hidden, password protected, encoded, or encrypted is criminal in nature. This information is important to criminal investigations, as the data which is hidden, password protected, encoded, or encrypted is more likely than not information for which criminals do not want others, especially law enforcement, to have access to, due to being criminal in nature. For example, a

suspect could place images and videos depicting child exploitation material in a password protected or hidden folder in order to obfuscate their illegal activity, or a suspect could place a password on a document which contains personal identification information of victims of identity theft.

I know from my training and experience that many digital devices are now using location-based information to assist users. This locational information is used to help find locations on a map, directions to a location, nearby points of interest, friends, and even reminders to name a few. There are numerous different ways that digital devices collect location information. Location based information is logged by default by the device's operating system when first setting up a digital device from a major manufacturer, such as Apple, Google, and Microsoft. While this can be disabled, generally the operating system of the device will still log locational based information, but that information will not be transferred to or utilized by the operating system manufacturer. Location based information is also logged by applications and software installed on digital devices. This can be done when a user manually enters location information, or automatically without the user's knowledge. This can be helpful in determining if a person was in a particular area at a particular date and time. It is very common for people to keep their cellular phones and/or other digital devices with them the majority of the time. Due to this, locations are consistently being logged by the operating system, software, and applications on the phone or device as to where the it was at specific points in time. This is true also for devices used by persons involved in criminal activity. For example, a suspect may use an application to search for addresses to meet with other persons for transactions of illegal items, or a suspect's digital device's operating system may log locations where a suspect was on a particular day which shows the suspect in the area of a crime at the time it was committed

I know from my training and experience that the preservation, acquisition and analysis of digital evidence can be a time consuming process. Each step can take days, weeks, or months depending on the complexity of the device. Due to the length of time needed for the preservation, acquisition and analysis, the date of service of the warrant will relate solely to the service of this warrant and not to the analysis of the listed devices.

The process of digital data preservation, acquisition and analysis is analogous to searching for a needle in a haystack; obtaining the haystack is akin to preservation and acquisition (seizure) of data, and carefully searching through the hay for the needle is akin to the analysis of data. A digital forensic examiner must first preserve and acquire (seize) the digital data to be analyzed, and only then can the digital forensic examiner analyze the entirety of the preserved data for information authorized by the search warrant.

Seize Digital Devices

I know that by simply looking at the physical aspects of a digital device, it is almost always impossible to determine the devices ownership, user-ship, and contents. Persons who use or have access to more than one digital device will more likely than not use multiple devices for similar reasons, even if those devices have an ideological separation between work and "play". It is not uncommon for persons using digital devices specifically for work purposes to conduct searches, research, or communication regarding their interests that are for personal reasons and not work related. Just as it is not uncommon for persons using digital devices specifically for reasons regarding their personal interests to conduct searches, research, or communication regarding their work. For these reasons and the ones described above (including backups, data synchronization, cloud data storage and access, and hidden information and data), it is more likely than not that all devices used by a person will contain data and information regarding that person's work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and/or associations. This is true also for persons involved in criminal

activity, where their work, activities, hobbies, interests, likes and dislikes, memorializations, achievements, and associations are criminal in nature.

I know that if people have secret data that exists on their digital device that they do not want others to know about, they will take steps in order to protect the discovery of that data. If those people are faced with a situation where others know that the secret data exists and may get access to that data, the person will take more steps to remove the possibility of others finding that secret data, such as deleting the data, moving the data, or destroying/disposing of the digital device itself. For example, if a person has information hidden on their phone detailing an extramarital affair (pictures, conversations, etc.) and believes their spouse will find out, that person will take steps to remove the possibility of that discovery from occurring. Or, if a person is planning a surprise party for a friend on a computer that the friend has access to, the person will take steps to ensure their friend will remain surprised. The same is true for persons involved in criminal activity. For example, if a suspect is aware that law enforcement is investigating them for a crime and evidence of that crime is contained on digital devices, the suspect is more likely than not to take steps to remove the possibility of discovery of that evidence

As discussed above, there are a number of items which categorize as digital devices. These devices range vastly in size, from small microSD cards which can hold millions of photos, videos, and documents, to cellular telephones which can fit in a pocket, to laptops that can fit in a backpack and travel well, to desktop computers that require a stationary desk, and everything in between. It is impossible to know without first searching a person's sphere of access, just how many digital devices they are in possession of and have access to. It is, however, more likely than not, that all of their digital devices have shared data and/or user interaction that is criminal in nature if any one device has data and/or user interaction that is criminal in nature, due to habits, common use of digital devices, backups, transfers, data synchronization, cloud data storage and access, and hidden information and data. It is also more likely than not that if a suspect knows that law enforcement is aware of their crimes, and the suspect knows that law enforcement is actively investigating those crimes, the suspect will take steps to remove the possibility of discovery of that evidence. For these reasons, it is imperative that digital devices capable of storing digital data of evidentiary value to a criminal investigation, which are under the possession and/or control of the suspect, be seized.

I know from my training and experience that a trained Digital Forensic Examiner has the ability to view data in a scientific, technical manner in order to make conclusions and determinations based upon the data from a digital device, such as user attribution and what data is of evidentiary value to the investigation. I know that this requires additional search authority which is not outlined within the confines of this affidavit, however, the devices must be seized before this can be completed.

Many times digital devices have proprietary power and/or data connection cables and without these cables it is impossible to connect to or power on the device. I have also found through my training and experience that by seizing operating logs, user notes, sticky notes or manuals, many of the usernames and passwords can in some instances be bypassed, which would otherwise restrict access to the data on the digital device if it was not able to be bypassed.

I know that digital data may be recovered from all forms of digital devices and storage media using a variety of digital forensic processes and techniques I also know through communication with digital forensic experts that the process of preserving (seizing) digital devices takes on many forms, and could include the disassembly of the digital device which can result in the digital device being rendered unusable in the manner in which it was designed to be used. Processes that allow for the forensic preservation and recovery of data by accessing the internal componentry of a digital device can successfully preserve and recover digital data when other forensic recovery techniques are not an

option. These forensic recovery and preservation techniques preserve and recover the data while making the device unusable, much like prying open a safe allows for the recovery of the contents of the safe but renders the safe itself unusable. Data recovery from digital media will always start with the least destructive forms of retrieval, but may require these more destructive methods that may render the device useless. I know through the communication with digital forensic experts that whatever method of data extraction is deemed necessary, the result will be an accurate representation of some or all of the available data from the device itself.

VII. Conclusion

This affidavit establishes probable cause to believe, and I do believe that the crime(s) of Murder, ORS 163.115 and Murder, ORS 163.115 has/have been committed and evidence of these crimes will be located in the location(s)/item(s) detailed in this affidavit.

Therefore, I pray that the court issue a warrant to search the aforementioned location(s)/item(s) described in this affidavit for evidence of the named crimes and to photograph, search, seize and/or analyze such evidence as described in the 'Item(s) to be Searched for and Seized' section of this affidavit.

Affiant

Subscribed and sworn to before me at 1237 am/pm on this 29 day of August, 2022.

Signature of Circuit Court Judge
Deschutes County

BETHANY FLINT
Printed Name of Circuit Court Judge
Deschutes County