UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

NORTH AMERICAN SCIENCE ASSOCIATES, LLC, a/k/a NAMSA, an Ohio limited liability company,

Plaintiff,

vs.

MICHAEL CONFORTI, PAMELA CONFORTI, and PHOENIX PRECLINICAL LABS, LLC, a Minnesota limited liability company,

Defendants.

Civil File No. 24-cv-00287

DECLARATION OF MARK LANTERMAN

I, Mark T. Lanterman, declare and state as follows:

1. I am the Chief Technology Officer of Computer Forensic Services ("CFS") located in Minneapolis, Minnesota.[1] CFS and I were retained by Dorsey & Whitney LLP as an expert witness in this action on behalf of Pamela Conforti.

2. I offer this declaration to respond to the certain findings of North American Science Associates, LLC ("NAMSA") expert, Mr. Kevin Faulkner. Specifically, this declaration is intended to describe Pam Conforti's copying and access of data originating from NAMSA from her personal devices since she separated from NAMSA on June 3, 2022. (*See* Compl. ¶ 97).

[1] Neither my compensation nor CFS's compensation is dependent upon the substance of my opinions or outcome of this case. Attached as **Exhibit A** is my CV, a list of cases in which I have testified in the last four years, as well as a list of articles I have published over the past 10 years.

I. Expert background & qualifications

3. Our firm specializes in the analysis of digital evidence in civil and criminal litigation. I have over 30 years of experience in computer forensics and cybersecurity. Prior to joining CFS, I was a sworn investigator for the United States Secret Service Electronic Crimes Task Force and acted as its senior computer forensic analyst.

4. I am certified by the United States Department of Homeland Security as a "Seized Computer Evidence Recovery Specialist," as well as certified in computer forensics by the National White-Collar Crime Center. Both federal and state court judges have appointed me as a neutral computer forensic analyst or special master.

5. I graduated from Upsala College with both a Bachelor of Science and a Master's degree in computer science. I completed my post graduate work in cyber security at Harvard University.

6. I have previously served as adjunct faculty of computer science for the University of Minnesota Technological Leadership Institute's Master of Science and Security Technologies program (MSST). I am a faculty member at the University of St. Thomas School of Law in Minnesota, and for the National Judicial College in Reno, Nevada. I have instructed members of the federal judiciary through the Federal Judicial Center in Washington, D.C.

7. I am a member of Working Groups 1 and 11 for the Sedona Conference, which is an institute dedicated to the advanced study of law. I serve on the Sedona Conference's Steering Committee on Artificial Intelligence and the Law.

8. I am currently appointed to the Arizona Supreme Court's Steering

Committee on Artificial Intelligence and the Courts.

9. I have previously provided training or delivered keynote addresses for the United States Supreme Court; the Eleventh Circuit Federal Judicial Conference; the Eighth Circuit Federal Judicial Conference; the Southern District of Georgia; the Western District of Tennessee; and several state judicial conferences. I delivered the keynote address at the Chief Justices' Conference in Newport, Rhode Island and at Georgetown Law School's advanced e-discovery conference.

10. I was appointed by the Minnesota Supreme Court to serve a maximum 6-year term as a member of Minnesota's Lawyers Professional Responsibility Board ("LPRB").

11. I am a co-author of the Minnesota State Bar's e-Discovery Deskbook, and I also write monthly articles for *Minnesota Bench & Bar* magazine.

12. CFS holds a corporate private detective license issued by the State of Minnesota Board of Private Detective and Protective Agent Services (License No. 2341).

13. CFS was awarded a Multiple Award Schedule contract (contract #47QTCA22D004L) for the 54151HACS (highly adaptive cybersecurity services) SIN by the General Services Administration (GSA). GSA awarded CFS the contract after a rigorous inspection and technical competence evaluation of knowledge, abilities, competency, policies, and procedures.

14. CFS is the exclusive, contracted computer forensic service provider for the Hennepin County Sheriff's Office; as well as the Metropolitan Airports Commission, also known as the Minneapolis/Saint Paul International Airport. I am a primary point-of-

contact for servicing these contracts on behalf of CFS.

15. As it relates to this action, I was deposed on April 8, 2024. My previous testimony is incorporated by reference.

I. Materials considered

16. Counsel for Ms. Conforti has shared with me, and I have reviewed, the following documents:

a. The complaint, filed on February 2, 2024 (Dkt. 1-2);

b. The February 2, 2024 declaration of Kevin T. Faulkner, and Exhibits 1-32, most of which were filed under seal;

c. The Court's Order of Referral, entered February 8, 2024 (Dkt. 54);

d. Protective Order, entered March 25, 2024 (Dkt. 111);[2]

e. The supplemental declaration of Kevin Faulkner, dated April 26, 2024 (Dkt. 172-173);

f. The declaration of Lisa Olson, dated April 26, 2024 (Dkt. 176-177)

17. In connection with my work, Ms. Conforti submitted multiple electronic devices for the purpose of forensic preservation and analysis. Table 1 below is intended to summarize the identifying information about those devices.

Description	**Make/Model**	**Serial Number**	**Date provided to CFS**
Pam Conforti's personal/work laptop	HP ZBook	5CG2192KR5	2/6/2024
Pam Conforti's external USB drive[3]	Seagate Model 2N1AP8-500	NACAN045	2/6/2024
Pam Conforti's iPhone	iPhone 12 Pro Max	F2LG1UEF0D3Y	2/14/2024

[2] I have executed an attestation to be bound by the protective order.
[3] *See* Faulkner Decl., Feb. 2, 2024 ¶ 15, describing the identifying information for the "First Pam Conforti External Drive."

Description	Make/Model	Serial Number	Date provided to CFS
Pam Conforti's "CABO" USB drive	SanDisk Cruzer 16-gigabyte USB drive	4C530001271111100284	2/23/2024

Table 1

18. Upon receipt of the devices listed above, CFS and I forensically preserved their data, and where necessary, obtained information necessary to decrypt them, and access/copy their contents (*e.g.*, passcodes and encryption keys).

19. With respect to the devices, and pursuant to the parties' agreement, I copied and transmitted the full forensic images (copies) of these devices to NAMSA's expert, Unit 42. (*See* Faulkner Supp. Decl., Apr. 27, 2024, Ex. 1).

20. In addition to submitting the full forensic images, CFS submitted "logical forensic images" of these devices to NAMSA's vendor, Consilio. As used here, a logical forensic image contains all files from Ms. Conforti's devices listed in Table 1, but does not include identified privileged content.

21. On April 29, 2024 and May 1, 2024, CFS received the forensic images created by Unit 42, including the forensic images of Ms. Conforti's previously issued NAMSA laptop and images of certain locations on NAMSA's server. Table 2 below describes information about these additional sources.

Description	Serial Number (if applicable)	Date received by CFS
Logical image constituting files from NAMSA's server (backup dated 2021-12-18)	N/A	May 1, 2024
Logical image constituting files from NAMSA's server (backup dated 2022-01-15)	N/A	May 1, 2024
Logical image constituting files from NAMSA's server (backup dated 2022-12-17)	N/A	May 1, 2024

Description	Serial Number (if applicable)	Date received by CFS
Pamela Conforti's NAMSA-issued laptop	2TK94603NN[4]	April 29, 2024

Table 2

II. Summary of Mr. Faulkner's analysis

22. As noted above, I have received the declarations of Plaintiff's expert, Kevin Faulkner. Mr. Faulkner has, in summary, concluded three things related to Ms. Conforti's retention and access of NAMSA data.

23. First, Mr. Faulkner has determined that Ms. Conforti attached USB devices to her NAMSA-issued laptop and copied and kept thousands of files. (*See* Faulkner Decl., Feb 2, 2024, ¶¶ 13-33, *see also* Faulkner Decl., Apr. 27, 2024 ¶ 63, Ex. 7).

24. Second, Mr. Faulkner has concluded that certain files, which may have originated at NAMSA were subsequently accessed using Ms. Conforti's personal devices. (*See* Faulkner Decl., Apr 27, 2024 ¶¶ 9, 65). More specifically, Mr. Faulkner has identified three (3) specific occasions that NAMSA files were accessed:

a. On January 11, 2024, a file called "S-GN-SP-001 Rev B ISO Sample Preparation 09.18.12.docx" and certain folders that are named consistent with NAMSA's naming conventions were accessed from an "unproduced" Kingston-branded USB drive. (*Id.* ¶¶ 43, 66)

b. On June 2, 2022, the day after the file was copied to Ms. Conforti's Seagate USB drive, Ms. Conforti accessed NAMSA's QuickBooks accounting and financial database file (*Id.* ¶ 67).

[4] *See* Faulkner Decl., Feb 2, 2024, Ex. 2.

c. On June 6 and 14, 2022, Ms. Conforti "accessed several .pst email storage files that she took from NAMSA."[5] (*Id.* ¶ 68).

25. Third, Mr. Faulkner identified 11 additional USB drives that were attached to Ms. Conforti's personal laptop, but that have not been produced for analysis. According to Faulkner, one of these devices contains NAMSA data. (*Compare with supra.* ¶ 11(a)).

III. Files that were copied to Ms. Conforti's external hard drive from her NAMSA computer, may not constitute only NAMSA data.

26. As noted above, Mr. Faulkner determined that Ms. Conforti copied and retained a total of 13 NAMSA Controlled Documents on her personal external hard drive.[6] (*See* Faulkner Decl., Apr. 27, 2024 Ex. 6).

27. As discussed by Mr. Faulkner, when files are opened and accessed, Windows often records information related to a user's interaction with files and folders, including those stored on an attached USB drive. For example, it is possible to determine whether a user "double-clicked" or opened files/folders stored on a USB device. When this occurs, it is also possible to determine the names of files and folders that exist/existed on an external USB drive. While the Controlled Documents identified by Faulkner are stored on the hard drive, there is no information to indicate that such

[5] "PST" is an acronym for "personal storage table" and is used by Microsoft Outlook to store email-related data.

[6] Ms. Conforti's Seagate external hard drive bears the serial number NACAN045. This external hard drive has been provided to CFS for preservation and analysis. As noted above, my office submitted the forensic image of this device to Mr. Faulkner for analysis.

NAMSA Controlled Document files were affirmatively accessed from Ms. Conforti's laptop.

28. Similarly, Mr. Faulkner identified 15,686 additional files that originated with NAMSA. (*Id.* Ex. 7). These files were "copied from NAMSA computer systems to [Ms. Conforti's] 5TB Seagate drive in 2022." (*Id.* ¶ 63).

29. According to Mr. Faulkner's Exhibit 7, even if the files originated from NAMSA's systems (*e.g.*, Ms. Conforti's NAMSA-issued laptop), they may not constitute NAMSA data. As just one example, Exhibit 7 lists thousands of photo and video files. Most of these files do not have any data to suggest that they represent NAMSA's property. On the contrary, the videos are stored within folders called, for example, "Pictures & Videos 2015 from IPhone [sic]" and "pams phone 3-25-18." In total, there are more than 8,000 photo and video files included in Mr. Faulkner's Exhibit—more than half of the total count of files that Ms. Conforti retained from her NAMSA computer.

30. In addition to thousands of photos and videos, substantial numbers of files are stored in folders that are also likely representative of personal information, including folders named "Personal," (more than 1,800 files) and "Taxes," (more than 2,600 files).

IV. Despite identifying substantial numbers of files, there are only three instances that Faulkner identifies to show that Ms. Conforti accessed NAMSA data.

31. As summarized above, there are three instances in which Ms. Conforti accessed files that ostensibly relate to or originated from, NAMSA.

a. A QuickBooks file was accessed on June 2, 2022.

32. First, Faulkner determined that QuickBooks workbook file was copied to Ms. Conforti's external hard drive on June 1, 2022. (*See* Faulkner Decl., Apr. 27, 2024 ¶ 67). This file is called "APSnetwork.QBW," where the extension QBW denotes that it is related to and contains QuickBooks financial/accounting information. This file is contained within a folder entitled "Quickbooks/APSNetwork."

33. There is no evidence to show that this file was accessed from Ms. Conforti's personal/Flexschema laptop after it was copied to the external hard drive. Indeed, and as noted by Mr. Faulkner, the file was last accessed on June 2, 2022. For this, Mr. Faulkner relies on the file system "last accessed" time. These dates are a reliable indicator of access when coupled with other facts or findings. This is because a file system last accessed time, standing alone, can be updated when a file is scanned by antivirus or indexed for searching.

34. In any event, whether the file was actually accessed/opened or not does not change the fact that the access on June 2, 2022 occurred using Ms. Conforti's NAMSA-issued laptop, not her personal laptop. (*See also* Faulkner Decl., Feb 2, 2024, Ex 4, showing APSnetwork.qbw accessed on June 2, 2022 from Ms. Conforti's personal hard drive using her NAMSA-issued computer). Indeed, on June 2, 2022 at 9:25 AM (CT), when the file was accessed, Ms. Conforti's personal laptop had not even been set up for her use.[7] Moreover, the earliest date that the external hard drive was connected

[7] Ms. Conforti's user profile on her laptop, "PamConforti" was not created until June 6, 2022.

to Ms. Conforti's personal laptop was June 6, 2022, which precludes the possibility that her personal computer was responsible for the update to the last accessed time associated with the Quickbooks file.

35. Lastly, I note that there is no evidence to indicate that Ms. Conforti copied the "APSnetwork.QBW" file from her personal external hard drive to other sources or computers. Indeed, the file does not exist on Ms. Conforti's personal laptop.

b. Ms. Conforti copied PST files, containing emails, to her personal computer.

36. A USB drive that Mr. Faulkner identifies as the "Second Pam Conforti External Drive" (bearing the serial number 0901be21a0047bd378602a7368341844084f75a10f6b64c2cc1640aa5045d31) was attached to Ms. Conforti's personal/FlexSchema laptop on June 14, 2022 at approximately 10:17 AM (Central Time) —four days after the device was attached to Ms. Conforti's NAMSA-issued laptop. (*See* Faulkner Decl. ¶ 26). June 14, 2022 is the only date on which the Second Pam Conforti External Drive was connected to her laptop.

37. On June 14, 2022 at approximately 10:25 AM, the file "exportofemail.pst" was copied from the Second Pam Conforti External Drive to her personal laptop. "PST" is an acronym for "personal storage table" and is used by Microsoft Outlook to store email-related data. The PST file was opened shortly after it was copied to Ms. Conforti's FlexSchema laptop.[8]

[8] This is established by the presence of a temporary file that is generated when a PST file is opened in Microsoft Outlook.

38. During my deposition, I testified about how my office was instructed to permanently destroy certain email data (including exportofemail.pst) after preserving Ms. Conforti's laptop. With respect to the "exportofemail.pst" file, on February 20, 2024, CFS permanently destroyed this file from Ms. Conforti's FlexSchema laptop, so as to remove Ms. Conforti's ongoing access to its contents.

39. Additionally, on February 20, 2024, CFS permanently destroyed a folder within Ms. Conforti's email mailbox titled "Emails/Folders to Export". This folder within Ms. Conforti's Outlook application contained approximately 2.6 GB of emails (according to Microsoft Outlook). CFS moved the "Emails/Folders to Export" folder to the "Deleted Items" folder within Outlook, and then emptied the Deleted Items, and compressed the PST file from within Outlook to minimize the chance that the deleted emails could be recovered.[9]

40. In addition to the folder within Outlook, CFS also identified and destroyed a folder, containing multiple PST files, that was stored on the Desktop of Ms. Conforti's laptop. The folder was called "Email PST Exports". This folder contained the following files:

- 4 Personal.pst
- 401K plan.pst
- All Emails.pst
- BMO.pst
- Buildings Lease.pst

[9] It should be noted that Ms. Conforti's laptop was connected to the internet during this operation. Therefore, actions taken while the laptop was online, and syncing should be reflected online. This helps ameliorate possible conflicts where data being removed while the device is offline is unintentionally restored when the device connects to the internet and synchronizes with the email account.

- Buildings.pst
- Buildout.pst
- Calendar.pst
- Closing Statement Analysis.pst
- Congratulations.pst
- Farewell.pst
- Fifth Third.pst
- Financial Package ERP.pst
- FlexSchema Company Set Up.pst
- FlexSchema IT SOPs.pst
- Last Month of Email.pst
- Lease Payoff.pst
- Lily.pst
- M & A.pst
- New Sikich Accounts.pst
- Personal.pst
- Pictures.pst
- PPP.pst
- Purchase Price Allocation.pst
- SBA Loan.pst
- Separation.pst
- Sikich.pst
- Transaction Payoff.pst
- Calendar.pst (stored within Ms. Conforti's Desktop folder)

41. CFS permanently destroyed the contents of the "Email PST Exports" folder, as well as the "Calendar.pst", and "exportofemail.pst" files on the Desktop. More specifically, CFS overwrote all data with one pass of random data, then a second pass of zeros. Understand that this action was intended to prevent ongoing access to the PST files by Ms. Conforti. Nothing from the forensic images that CFS captured (and sent to NAMSA's expert) were affected by these actions.

c. Ms. Conforti accessed a single file on January 11, 2024 from a USB drive.

42. There is one USB drive that contained files named in a manner consistent with NAMSA data that was attached to Ms. Conforti's laptop on January 11, 2024. (*See*

Faulkner Decl., Apr. 27, 2024 ¶ 7). More specifically, these documents were accessed from a Kingston-branded USB drive, bearing the serial number 0013729945E6EAC095130087.

43. On January 11, 2024 at approximately 4:37 PM (CT), this Kingston USB drive was attached to Ms. Conforti's laptop. Thereafter, Ms. Conforti's laptop was used to access eight (8) folders that are named consistent with NAMSA's naming conventions, and a single document stored within those folders. Table 3 below summarized information about the accessed files.

Folder/File Accessed	**File/Folder Name**	**Date Created on USB drive**	**Date Modified**
01/11/2024 04:38:12 PM	D:\Biocompatibility\Final Report Templates	10/03/2012 04:22:34 PM	N/A
01/11/2024 04:38:59 PM	D:\In-Life Research - Biocompatibility - Animal Care (S-IL-BC-AC)	10/03/2012 04:59:30 PM	N/A
01/11/2024 04:39:01 PM	D:\In-Life Research - Biocompatibility - Operations (S-IL-BC-OP)	10/03/2012 04:59:48 PM	N/A
01/11/2024 04:39:04 PM	D:\In-Life Research - Toxicology (S-IL-TX)	10/03/2012 05:00:24 PM	N/A
01/11/2024 04:39:05 PM	D:\In-Vitro Testing - General (S-IV-GN)	10/03/2012 05:02:16 PM	N/A
01/11/2024 04:39:07 PM	D:\In-Vitro Testing - Cytotoxicity Operations (S-IV-CY-OP)	10/03/2012 05:02:16 PM	N/A
01/11/2024 04:39:21 PM	D:\General - Sample Prep (S-GN-SP)	10/03/2012 04:58:12 PM	N/A
01/11/2024 04:39:21 PM	D:\General - Sample Prep (S-GN-SP)\S-GN-SP-001 Rev B ISO Sample Preparation 09.18.12.docx	10/03/2012 04:58:11 PM	09/13/2012 03:09:54 PM
01/11/2024 04:39:54 PM	D:\In-Vitro Testing - Hemocompatibility (S-IV-HE-OP)	10/03/2012 05:02:16 PM	N/A

Table 3

44. As indicated above, the accessed document and folders were created in 2012. This fact is notably absent from Mr. Faulkner's declaration. The activity timeline

outlined above is consistent with an individual previewing the content of the USB drive, as there is nothing to indicate that Ms. Conforti accessed files from the majority of folders that are known to have existed on the USB drive.

45. Two minutes and forty seconds after the USB drive was attached, and the contents previewed, it was unplugged at 4:40 PM and was not subsequently reconnected.

V. There is no evidence to suggest that NAMSA data existed on 9 of the 11 "unproduced" USB drives attached to Pam Conforti's laptop.

46. In his supplemental declaration, Mr. Faulkner identified a total of 11 "unproduced." devices that were previously attached to Ms. Conforti's personal/Flexschema laptop. Of these 11 devices, seven (7) were attached on a single date—January 11, 2024. On that date, the seven USB drive were attached for limited periods of time.

47. Table 4 below is intended to summarize information about the unproduced USB drives, including the durations that it was attached, and the identification of files that were accessed from them.

Serial Number and Device Name	**Last Connected**	**Duration**	**Files Accessed**
0901be21a0047bd378602a7368341844084f75a10f6b64c2cc1640aa5045d31 […] USB SanDisk 3.2Gen1	06/14/2022 04:42:32 PM	N/A	This USB drive was identified by Mr. Faulkner and contained the "exportofemail.pst" file discussed *supra*. The only date that this device was attached was June 14, 2022.

Serial Number and Device Name	**Last Connected**	**Duration**	**Files Accessed**
AA6TZHJP30XPWB1T Lexar USB Flash Drive USB Device	10/14/2023 08:16:10 PM	0:01:49	This device was only connected on October 14, 2023. Two video files were accessed from this device previously: • D:\temp\fe62b88aa06e05e44e76d6f27a6c5d20.mp4 • D:\._fe62b88aa06e05e44e76d6f27a6c5d20.mp4
2212121017383944515607 General UDisk USB Device	10/24/2023 03:45:52 PM	0:21:10	This device was only connected on October 24, 2023. Two video files were accessed from this device previously: • D:\Donna_L._Maul_Spencer.mp4 • D:\.Trashes\501\Beverly_Bev_Vilberg.mp4
058F84688461 Generic-SD/MMC USB Device	01/04/2024 08:58:38 AM	29:11:24	This is highly like an SD card reader. There is nothing to affirmatively indicate that files were accessed from this device.
001CC0EC2F39EAC095CB0042 Kingston DT 100 G2 USB Device	01/11/2024 04:37:20 PM	0:01:18	There is nothing to affirmatively indicate that files were accessed from this device. I note that the only date that it was connected was January 11, 2024.
0013729945E6EAC095130087 Kingston DT 100 G2 USB Device	01/11/2024 04:40:22 PM	00:02:40	This device was only attached on January 11, 2024. This device ostensibly contained NAMSA data. (*See supra.*).

Serial Number and Device Name	**Last Connected**	**Duration**	**Files Accessed**
SNDK2F07152 A44707407 SanDisk Cruzer Micro USB Device	01/11/2024 04:45:21 PM	00:03:08	This device was only attached on January 11, 2024, and used to access two photos: • D:\img112.jpg • D:\img116.jpg
07A609030AA EB193 Memorex Travel Drive CL USB Device	01/11/2024 04:47:06 PM	00:00:33	There is nothing to affirmatively indicate that files were accessed from this device. I note that the only date that it was connected was January 11, 2024.
60A44C3FAC DBF160796E0 CF6 Kingston DataTraveler 3.0 USB Device	01/11/2024 04:49:21 PM	00:01:01	This device was only attached on January 11, 2024, and used to access three folders: • D:\Job Documents • D:\Training Videos • D:\Handouts
0400121708132 0202042 SanDisk Cruzer Glide USB Device	01/11/2024 04:51:30 PM	00:00:59	There is nothing to affirmatively indicate that files were accessed from this device. I note that the only date that it was connected was January 11, 2024.
6&1fa7b3ee USB MEMORY BAR USB Device	01/11/2024 04:51:46 PM	00:11:14	There is nothing to affirmatively indicate that files were accessed from this device. I note that the only date that it was connected was January 11, 2024.

Table 4

48. As illustrated by Table 4 above, only two (2) of the "unproduced" USB devices may contain NAMSA data. That is, the device with the serial number beginning "0901be21a0047" contained a single PST file provided to Ms. Conforti by NAMSA IT;

and the device bearing the serial number 0013729945E6EAC095130087 contained several folders consistent with NAMSA's naming conventions that were copied to it in 2012.

49. As an aside, there is nothing to indicate or suggest that Ms. Conforti attached Dr. Conforti's external hard drive (serial number NABAFEDS) to her laptop at any time.

50. I respectfully reserve the right to supplement or amend this declaration should additional information be made available, or if additional details are requested.

I declare under penalty of perjury under the law of the United States that the foregoing is true and correct.

Executed on: May 24, 2022 in Hennepin County, Minnesota.

Mark Lanterman

EXHIBIT A

ComputerForensic Services

Mark Lanterman
Chief Technology Officer

Office
800 Hennepin Avenue
5th Floor
Minneapolis, MN 55403

Phone
(952) 924-9220

Fax
(952)924-9921

Email
mlanterman@compforensics.com

Web
www.compforensics.com

Professional Biography

Mark has over 30 years of experience in digital forensics, e-discovery, and has provided education and training to a variety of audiences. Prior to founding Computer Forensic Services in 1998, Mark was a sworn investigator with the United States Secret Service Electronic Crimes Task Force. Both federal and state court judges have appointed Mark as a neutral computer forensic analyst.

Mark was appointed by the Minnesota Supreme Court for two consecutive three-year terms as a member of the Minnesota Lawyers Professional Responsibility Board, during which he also actively contributed to its Rules & Opinion Committee.

Mark frequently provides training within the legal community, including presentations for the United States Supreme Court, Georgetown Law School, the 11th Circuit Federal Judicial Conference, the 8th Circuit Federal Judicial Conference, the American Bar Association, the Federal Bar Association, the Sedona Conference, and the Department of Homeland Security, among others.

Mark has provided training for federal judiciary members via the Federal Judicial Center in Washington, D.C. Additionally, he serves as faculty at the National Judicial College. Mark is a professor in cybersecurity at the Saint Thomas School of Law. Mark is a member of the Sedona Conference Working Groups 1 and 11, where he is recognized as a "dialogue leader" on the judicial branch's adoption of Artificial Intelligence. Further, Mark was appointed by the Arizona Supreme Court to its judicial steering committee for the implementation of Artificial Intelligence.

Education and Certifications

Upsala College – B.S. Computer Science; M.S. Computer Science

Harvard University – Cybersecurity

Department of Homeland Security – Federal Law Enforcement Training Center
Seized Computer Evidence Recovery Specialist

National White-Collar Crime Center – Advanced Computer Forensics

Publications

Co-author of the *E-Discovery and Forensic Desk Book*

Regular columnist for *Bench & Bar* magazine

ComputerForensic Services

Previous Testimony List – Mark Lanterman

- *Raymond James & Associates, Inc. et al. v. Piper Sandler et al.*, 2:23-CV-02644 (W.D. Tenn.)
- *Piper Sandler Companies v.* Gonzalez
- *State v. James Nyonteh*, 27-CR-22-5940 (Henn. Co., Minn)
- *State v. Zhaaboshkang Bush,* 04-CR-22-2661 (Beltrami Co., Minn)
- *Lauren Ellison v. JM Trucking, et al.,* 2023CI16452 *(*Bexar Co., Texas)
- *State v. Gary Otero, 52-CR-23-57 (*Nicollet Co., Minn.)
- *Mayo Foundation for Medical Education & Research v. Knowledge to Practice, Inc.,* 21-CV-1039 (D. Minn.)
- *Wilbur-Ellis Company LLC v. J.R. Simplot et al. (D. South Dakota)*
- *Universal Power Marketing, et al. v. Sara Rose,* 82-CV.20-2812 (Henn. Co., Minn.)
- *TCIC, Inc. v. True North Controls, LLC, et al.,* 27-CV-22-3774 (Henn. Co. Minn.)
- *MHL Custom, Inc. v. Waydoo USA, Inc, et al.,* 21-CV-0091 (D. Delaware)
- *Tumey LLP, et al. v. Mycroft, Inc., et al.,* 4:21-CV-00113 (W.D. Mo.)
- *A'layah Le'vaye Horton v. Greenway Equipment Co., Inc. et al.,* 20MI-CV00562 (Miss. Co., Missouri)
- In the Marriage of: Beals and Beals, 12-FA-21-235 (Chippewa Co., Minn.)
- *Warren, et al. v. ACOVA, Inc., et al.,* 27-CV-18-3944, (Henn. Co., Minn.)
- *Hagen v. Your Home Improvement, LLC, et al.*, 73-cv-21-2067, (Sterns Co. Minn.)
- *State of Minnesota v. Raku Sushi & Lounge Inc.,* 27-CR-21-8730, (Henn. Co., Minn.)
- *Jane Doe, et al. v. Independent School District 31,* 20-CV-00226, (D. Minn.)
- Galan v. Munoz, et al., 2019-CI-19143, (Bexar Co., Texas)
- *Vision Industries Group, Inc. v. ACU Plasmold, Inc., et al.,* 2:18-CV-6296, (D. N.J)
- *Troutman v. Great American Hospitality, LLC,* 19-CV-878, (Stanley Co., N. Carolina)
- *Baxter Insurance Group of Agents, et al. v. Woitalla et al., 27-CV-20-16685,* (Henn. Co. Minn.)

- *Sweigart v. Patten, et al.,* 5:21-cv-00922, (U.S. Dist Ct. E.D. Penn.)
- *Sarah Hoops v. Solution Design Group, Inc.,* 27-CV-20-11207, (Henn. Co. Minn.)
- *Stephanie Ramos v. Lazy J Transport, et al.,* 2018CI21594, (Dist Ct. Bexar Co., Texas)
- *Schwan's Company, et al. v. Rongxuan Cai, et al.,* 0:20-SC-2157, (U.S. Dist. Ct. Minn.)
- *Michael D. Tewksbury, as Guardian ad Litem for Miles Chacha and Lulu Kerubo Simba v. PODS Enterprises, LLC, et al.,* 62-CV-20-4209, (Ramsey Co., Minn.)
- *RG Golf v. The Golf Warehouse, 19-CV-00585* (U.S. Dist. Ct. Minn.)
- *Dunn v. PSD LLC, et al.,* 02-CV-20-4504, (Anoka Co., Minn.)
- *Chambers, et al. v. B&T Express, et al.,* 19-CI-00790, (Franklin Cir. Ct. Ky. 2d Div.)
- *Natco Pharma Ltd. V. John Doe,* 21-cv-00396-ECT-BRT, (U.S. Dist. Ct. Minn.)
- *Kimberly Clark, et al. v. Extrusion Group, et al.,* 1:18-cv-04754-SDG, (U.S. Dist. Ct. N.D. Ga.)
- *PalatiumCare Inc. v. Notify, LLC, et al.,* 2021-cv-000120, (Sheboygan Co., Wis.)
- *State of Nebraska v. Jeffrey Nelson,* CR21-19, (Saunders Co., Nebraska)
- *Lutzke v. Met Council,* 27-CV-19-14453, (Henn. Co. Minn.)
- *Rivera et al., v. Hydroline, et al.,* DC-19-143, (Dist. Ct. Duval Co, Texas).
- *Coleman & Hartman, et al. v. iAMg, et al.,* 16CV317, (Cir. Ct. Polk Co Wis.)
- *Mixon v. UPS, et al., 2019-CI-13752,* (Dist Ct. Bexar Co., Texas)
- *Goodman v. Goodman,* 27-DA-FA-21-672, (Henn. Co. Minn.)
- *Shaka v. Solar Partnership,* 27-CV-20-12474, (Henn. Co. Minn.)
- *Patel Engineering Ltd. V. The Republic of Mozambique,* UNCITRAL PCA: 2020-21.
- *Estate of Rima Abbas v. ABDCO,* (19-CI-1315), (Fayerette Cir. Ct. Ky. 4th Div.)
- *State of Nebraska v. Jeffrey Nelson,* CR21-19, (Saunders Co., Nebraska)
- *Riccy Mabel Enriquez-Perdomo v. Richard A. Newman, et al.,* 3:18-CV-549, (U.S. W.D. Kentucky)
- *United States v. Alakom-Zed Crayne Pobre,* PX-19-348, (U.S. Dist. Maryland)
- *Lewis v. Northfield Savings Bank, et al.,* 295-5-19-WNCV, (Vermont, Sup. Ct., Washington Div.)

- *State of Minnesota v. Thomas James Crowson,* 13-CR-20-325, (Chisago Co., Minn.)
- *Vimala et al., v. Wells Fargo, et al.,* 3:19-CV-0513, (U.S. M.D. Tenn.)
- In re: Estate of Anthony Mesiti, 318-2017-ET-00340, N.H. 6th Cir. Probate Division.
- Ernie's Empire, LLC, et al. v. Burrito & Burger, Inc., et al., 82-CV-20-28, (Wash. Co., Minn.)
- *Sol Brandys v. Wildamere Capital Management LLC,* Case No.: 27-CV-18-10822, (Henn. Co., Minn.)
- *State of Minnesota v. Yildirim*, 27-CR-19-7125, (Henn. Co., Minn.)
- *Jabil v. Essentium, et al.,* 8:19-cv-1567-T-23SPF, (M.D. Fla.)
- Lifetouch National School Studios Inc. v. Walsworth Publishing Company, et al., (U.S. Dist. Conn.)
- *Motion Tech Automation, LLC v. Frank Pinex*, Case No.: 82-CV-18-5202, (Wash. Co., Minn.)
- *Lundin v. Castillo, et al.*, Case No.: 2019-CV-000452, (Walworth Co., Wis.)
- *Yun v. Szarejko-Gnoinska, et al.,* 27-PA-FA-13-967, (Henn. Co., Minn.)
- *Jonas Hans v. Belen Fleming*, Case No.: 27-PA-FA-13-967, (Henn. Co., Minn.)
- *Daniel Hall, et al. v. Harry Sargeant III*, 18-cv-80748, (S.D. Fl.)
- *Miller v. Holbert, et al.,* Case No.: 48-CV-15-2178, (Mille Lacs Co., Minn.)
- *Strohn, et al. v. Northern States Power Company, et al*., 18-cv-1826, (U.S. Dist. Ct. Minn.)
- Stamper, et al. v. Highlands Regional Medical Center, Case Nos.: 11-CI-1134 & 12-CI-00468, (Commonwealth of Kentucky, Floyd Cir. Co., Div. I).
- *Patterson Dental Supply, Inc. v. Daniele Pace*, Case No.: 19-cv-01940-JNE-LIB, (U.S. Dist. Ct. Minn.)
- *Ryan Rock v. Jonathan Sargent and The Sargent Group, Inc. d/b/a Todd & Sargent, Inc.,* LACV050708, (Story Co., Iowa)
- Oscar Alpizar v. Eazy Trans, LLC, et al., 2018CI00878, (Bexar Co., Texas)
- *MatrixCare v. Netsmart*, Case No.: 19-cv-1684, (D. Minn.)
- *State of Minnesota v. Nathan Roth*, Case No.: 80-CR-18-1007, (Wadena Co., Minn.)
- *Parisi v. Wright*, Case No.: 27-CV-18-5381, (Henn. Co., Minn.).
- *Lloyd C. Peeoples, III v. Carolina Container, LLC*, 4:19-cv-00021 (N.D. Georgia)
- *Sandra Wolford, et al. v. Bayer Corp*., et al., 16-CI-907, 17-CI-2299, Pike Cir. Ct. Div. I, Kentucky)

- *BuildingReports.com, Inc. v. Honeywell International, Inc.,* Case No.: 1:17-cv-03140-SCJ, (N.D. Ga.)
- *Evan D. Robert and Dr. Kerry B. Ace v. Lake Street Cafeteria, LLC, et al.,* Case No: 27-CV-17-18040, (Henn. Co., Minn.)
- *State of Minnesota v. Andrew Seeley,* 14-CR-17-4658, (Clay Co., Minn)
- *State of Minnesota v. Stephen Allwine*, 82-CR-17-242, (Wash. Co., Minn.)

ComputerForensic Services

Publications List – Mark Lanterman

Bench & Bar of Minnesota

Ransomware and federal sanctions, January/February 2024

Biden issues ambitious executive order on AI, December 2023

The CSRB weighs the lessons of Lapsus$, November 2023

Deepfakes, AI, and digital evidence, October 2023

Protecting our judges, September 2023

CISO Beware: Cyber accountability is changing, August 2023

ChatGPT: The human element, July 2023

This article is human-written: ChatGPT and navigating AI, May/June 2023

The shifting emphasis of U.S. cybersecurity, April 2023

Gloves off: The upcoming national cybersecurity strategy, March 2023

Thinking about the future of cyber insurance, January/February 2023

Ransomware and counteracting the interconnected risks of the IoT, December 2022

Executive Order 22-20 and Minnesota's growing cybercrime rates, November 2022

Social engineering or computer fraud? In cyber insurance, the difference matters, October 2022

The Cyber Safety Review Board's first report and the impact of Log4j, September 2022

What critical infrastructure efforts can teach us about cyber resilience, August 2022

How the American Choice and Innovation Online Act may affect cybersecurity, July 2022

Smishing attacks and the human element, May/June 2022

Still on the defensive, More on the Missouri website vulnerability investigation, April 2022

What we can already learn from the Cyber Safety Review Board, March 2022

The Log4j vulnerability is rocking the cybersecurity world. Here's why., January/February 2022

On the defensive: Responding to security suggestions, December 2021

Go fish? Proportionality revisited, November 2021

Mailbag: Cybersecurity Q+A, October 2021

The NSA advisory on brute force attacks, September 2021

Security is a team game, August 2021

Improving national cybersecurity, July 2021

Apple's new iOS strikes a blow for data privacy, May/June 2021

Geofence warrants, The battle is just beginning, April 2021

Ransomware and federal sanctions, March 2021

The SolarWinds breach and third-party vendor security, February 2021

Considerations in cloud security, January 2021

Deciding when to use technology-assisted review, December 2020

How to avoid an old scam with a new twist, November 2020

Your back-to-school tech brush-up, October 2020

The Twitter breach and the dangers of social engineering, September 2020

Cyber risk: Is your data retention policy helping or hurting?, August 2020

Cyber riots and hacktivism, July 2020

Working from home and protecting client data, May/June 2020

Cybersecurity in pandemic times, April 2020

Business continuity and coronavirus planning, March 2020

Doxxing made easy: social media, March 2020

Taking responsibility for your cybersecurity, February 2020

Beyond compliance: Effective security training, January 2020

Doxxing redux: The trouble with opting out, December 2019

Proportionality and digital evidence, November 2019

AI and its impact on law firm cybersecurity, October 2019

Too secure? Encryption and law enforcement, September 2019

Security, convenience and medical devices, August 2019

Physical security should be part of your incident response plan, July 2019

"Papers and effects" in a digital age, pt II, May/June 2019

Security considerations for law firm data governance, April 2019

Third-party vendors and risk management, March 2019

The Marriott breach: four years?, February 2019

"Papers and effects" in a digital age, co-authored with Judge (Ret.) Rosenbaum, January 2019 (Republished in The Computer & Internet Lawyer)

The Chinese spy chip scandal and supply chain security, December 2018 (Republished in The Computer & Internet Lawyer)

Don't forget the inside threat, November 2018

Cyberattacks and the costs of reputational harm, October 2018

Fair elections and cybersecurity, September 2018

E-discovery vs. forensics: Analyzing digital evidence, August 2018

Social media and managing reputational risk, July 2018

Managing Cyber Risk: Is cyber liability insurance important for law firms?, May/June 2018 (Republished in The Computer & Internet Lawyer)

Social engineering: How cybercriminals capitalize on urgency, April 2018

Stephen Allwine: When crime tries to cover its digital tracks, March 2018

Is the Internet of Things spying on you?, February 2018

#UberFail, January 2018

Ransomware: To pay or not to pay?, December 2017

How digital evidence supported gerrymandering claims, November 2017

Facial recognition technology brings security & privacy concerns, October 2017

Putting communication and clients first in digital forensic analysis, September 2017

Digital evidence: New authentication standards coming, August 2017

Your Personal Data – Or is it? Doxxing and online information resellers pose threats to the legal community, May/June 2017

What You Don't Know Can Hurt You: Computer Security for Lawyers, March 2014

Minnesota Lawyer

Phishing, vishing and smishing – oh, my!, January 2018

Equifax was unprepared for a data breach, September 2017

Cybersecurity and forensic application in cars, July 2017

Preventing 'spear-phishing' cyber attacks, May 2017

Opting out when private information goes public, March 2017

Are fingerprints keys or combinations?, February 2017

Digital Forensics and its role in data protection, February 2017

Acknowledge the security issues, December 2016

Modern life is driven by the internet of things, November 2016

Are medical devices vulnerable to hackers?, October 2016

Digital evidence as today's DNA, September 2016

Colorado Lawyer

Is Emailing Confidential Information a Safe Practice for Attorneys?, July 2018 (Republished in The Journals & Law Reviews database on WESTLAW)

International Risk Management Institute, Inc. (IRMI)

Considerations on AI and Insurance, December 2023

Data Retention Policies as Proactive Breach Mitigation, October 2023

Cyber-Risk Management in the Age of ChatGPT, June 2023

Cyber-Security Considerations for Employee Departures, April 2023

Cyber Safety Review Board on Lapsus$, December 2022

Apple Vulnerabilities and Staying Apprised of Current Cyber Threats, September 2022

Evolving Threats? Assess and Update Security Measures, June 2022

Cyber Security and the Russian Invasion of Ukraine, April 2022

Thoughts on the FBI Email Compromise—and Lessons Learned, January 2022

Ransomware, National Cyber Security, and the Private Sector, October 2021

Standardization Matters in Establishing a Strong Security Posture, June 2021

Third-Party Vendor Risk Management, March 2021

The Importance of (Remote) Security Culture in Mitigating Risks, December 2020

Security from Home: Continuing to Work and Learn Amid COVID-19, September 2020

Operational Risk Revisited in the Wake of COVID-19, June 2020

Cyber Threats and Accounting for Operational Risk, March 2020

Human Aspect of Incident Response Investigations, January 2020

The Impact of Digital Incompetency on Cyber-Security Initiatives, September 2019

Communication in Responding to Cyber Attacks and Data Breaches, June 2019

Cyber Security and Resilience, January 2019

Leadership in Developing Cultures of Security, September 2018

Real-Life Consequences in a Digital World: The Role of Social Media, July 2018

Some Thoughts on the Dark Web—and How it Affects You, March 2018

Personal Information and Social Media: What Not to Post, September 2017

Managing Doxxing-Related Cyber Threats, July 2017

Understand the Layers of Cyber-Security and What Data Needs Protecting, March 2017

Learn about the Internet of Things: Connectivity, Data, and Privacy, January 2017

Assessing Risk and Cyber-Security, September 2016

SCCE The Compliance & Ethics Blog

The Components of Strong Cybersecurity Plans: Parts 1-5, 2017

Prevention Is the Best Medicine, August 2016

Lawyerist

Detection: The Middle Layer of Cybersecurity, April 2017

Don't Be Too Hasty! What to Do When an Email Prompts You to Act Quickly, February 2017

How to Avoid Spoofing, Spear Phishing, and Social Engineering Attacks, October 2016

Law Practice

The Dark Web, Cybersecurity and the Legal Community, July/August 2020

Captive International

COVID-19 and the importance of the cyber captive, April 2020

Attorney at Law Magazine

The Digital Challenges of COVID-19, June 2020

E-Discovery Deskbook

Chapter Thirteen "Forensic Experts—When and How to Leverage the Talent" co-authored with John M. Degan Briggs and Morgan, P.A.

The Complete Compliance and Ethics Manual 2022

Cybervigilance in Establishing Security Cultures