



SPECIAL COUNSEL

Report

In the Matter of:

Stein, et al v. Needle, et al

Project Name: Stein, et al v. Needle, et al
Project Number: 228330
Examiner: John R. Clingerman, CFCE
Report Date: August 27, 2021
Revision Date: September 1, 2021
Addendum Added: October 31, 2021

Special Counsel, Inc.
4350 W. Cypress St.
Suite 750
Tampa, FL 33607

Table of Contents

I. Company Background.....	3
II. Personal Statement	3
III. Project Background and Tasks.....	4
IV. Sources of Information	5
V. Timeline of Events	7
VI. Conclusions.....	8
VII. Recommendations for Remediation	10
Addendum.....	13
Updated Recommendations for Remediation.....	20
Exhibit A.....	21

CONFIDENTIAL

I. Company Background

Special Counsel, Inc. (SCI) is an international provider of electronic discovery, digital forensics, information management, and litigation support services to law firms and corporations. SCI's Forensic Services Group specializes in preservation, collection, handling, analysis and reporting of electronically stored information ("ESI") for use in connection with or anticipation of litigation or other investigations.

II. Personal Statement

My name is John R. Clingerman, and I have been employed by D4, LLC (D4) for over 14 years, the last five of which were spent under the ownership of Special Counsel, Inc. (SCI) with responsibilities that include performing computer forensic examinations. Additionally, I was a full-time police officer for 24 ½ years, the last fourteen of which I spent as a Police Investigator with responsibilities involving the investigation of all types of felony crimes including the investigation of computer related criminal activity. My computer forensic trainings have been with the National White-Collar Crime Center (NW3C), International Association of Computer Investigative Specialists (IACIS), Guidance Software, Access Data Corporation and Sumuri Forensics. I am a Certified Forensic Computer Examiner (CFCE), a Certified Electronic Evidence Collection Specialist (CEECS), a Certified Mobile Device Examiner, a Certified Police Officer in the State of New York, and a Licensed Private Investigator in the States of New York, Texas and Florida. My criminal trial testimony experience is extensive and spans my entire law enforcement career during which I testified hundreds of times in federal, state, and local courts. During the last 14 years with D4/SCI, my testimony experience has consisted of:

- For Civil Plaintiff – August 2021 at deposition for the Matter Gregory M. Hall Trust Agreement, Court File No. 2018-383,234-TV, Oakland County Probate Court, Michigan
- For Civil Plaintiff – October 2020 at deposition for Commodity Solutions, Inc. vs. Zane Abner and Ethan Bruland Roberts, Case No. CI 16-312 in the District Court of Platte County Nebraska.
- For Plaintiff – July 2020 at hearing for HBW vs. Gentry, et al., Civil Action No. 1:20-cv-00395-RBJ, in the United States District Court for the District of Colorado
- For Plaintiff – July 2020 at deposition for HBW vs. Gentry, et al., Civil Action No. 1:20-cv-00395-RBJ, in the United States District Court for the District of Colorado
- For Plaintiff – April 2019 at deposition for Gene Stamper and Alicia Stamper vs. Northern Arizona Health Care Corporation, No. CV2016-00259, Superior Court, Coconino County, Arizona

- For Criminal Prosecution – May 2018 at trial for People of the State New York vs. Robert DePalo, Supreme Court, Criminal Term Part 59, Indictment # 04150-2015.
- For Civil Defendant – February 2017 at deposition for Office Depot, Inc. et al vs. Roberts, Case No. 1:2016cv04234 in the New York Southern District Court.
- For Civil Plaintiff – April 2016 at hearing In the Matter of the Estate of William R. Nunz, File No. 2012-4075 in the Surrogate’s Court of Erie County, Buffalo, NY.
- For Civil Defendant – October 2013 at arbitration hearing for Kevin Wailes v. Tel-Networks, USA, LLC, JAMS Arbitration No. 1425013444 in Manhattan, NY.
- For Civil Defendant – September 2013 at trial for Michael Weidner vs. Lisa Six Weidner, Index No. 9621/2012 in the State Supreme Court, Monroe County, NY.
- For Civil Plaintiff - June 2012 at second deposition for American Builders & Contractors Supply Co., Inc. vs. Roofers Mart, Inc., Bernard S. Miller Jr., Michael L. Burger, Lucas Y. Abbott, Mark E. Lineberry, Daniel Woodall, Steven G. Declue, and John E. Slattery, Case No. 1:11-cv-00019 CEJ in the United States District Court for the Eastern District of Missouri
- For Civil Defendant – May 2012 at deposition for Juan and Ramona Medina vs. Pile Trucking, Inc., Case No. CV-11-06329 GHK in the United States District Court for the Central District of California Western Division
- For Civil Plaintiff - September 2011 at first deposition for American Builders & Contractors Supply Co., Inc. vs. Roofers Mart, Inc., Bernard S. Miller Jr., Michael L. Burger, Lucas Y. Abbott, Mark E. Lineberry, Daniel Woodall, Steven G. Declue, and John E. Slattery, Case No. 1:11-cv-00019 CEJ in the United States District Court for the Eastern District of Missouri Southeastern Division
- For Civil Defendant - July 2010 at trial for Haute Couture vs. Continental Casualty Company, Case No. 4:09-cv-809 JLH in the U.S. District Court, Eastern District of Arkansas, Western Division
- For Criminal Prosecution - October 2008 at Grand Jury New York County, NY for State of NY vs. Testwell, Inc.
- Generated dozens of affidavits that were subsequently submitted to various state and federal district courts

Attached to this report is my curriculum vitae titled *Exhibit A*.

III. Project Background and Tasks

On November 3, 2020, Steven Teppler of the law firm Mandelbaum Salsburg P.C. consulted with SCI to determine if SCI could assist with an investigation and act as a court appointed forensic computer expert and special master in a civil proceeding involving Dr. Barry D. Stein and Fairfield Anesthesia Associations, LLC (FAA) vs. Needle | Cuda: Divorce & Family Law

(Needle | Cuda). The need for an investigation came about during the divorce proceeding of Barry D. Stein, represented by the law firm Reich & Truax, PLLC (Reich & Truax) and Jennifer Stein, represented by Needle | Cuda Law. At issue was the alleged unauthorized download of data from a home computer in the Stein home by Jessica Calise of Needle | Cuda that included 800+ FAA patient and employee records within part of the downloaded data. Additionally, it's alleged that the downloaded data was later transferred to a Needle | Cuda Dropbox account and a link to the Dropbox site subsequently sent via email to various parties.

A court order issued on 11-04-2020 by Judge Vanessa L. Bryant of the U.S. District Court, District of Connecticut states in part: ***In this examination, the special master will be required to identify any patient and employee information downloaded from Dr. Stein's FAA issued computer, identify whether such information was downloaded and stored, determine whether it was further disseminated, and if so, where. After receiving appropriate relief from the Superior Court, the special master will be required to validate or execute the permanent deletion of the confidential patient and employee information.***

On November 18, 2020 the parties reached an agreement that SCI would be the designated forensic computer expert and special master in the matter. The tasks outlined via court order (noted above) were used as the guide for SCI to function as the forensic computer expert and special master. SCI's approach to accomplish the tasks was to review transcripts and depositions, access and forensically image Needle | Cuda's Dropbox and an external hard drive, access and forensically image the Stein home computer, review emails with the Dropbox link that were disseminated to various persons, and interview persons with knowledge or a direct connection to the download process and dissemination events.

This report addresses the FAA patient and employee records that were copied from the Stein home computer, the locations the records were transferred to, who/how transfers were performed, the current storage locations of the records, and recommendations to the court for relief, i.e., deletion of the records from the specified locations and/or preservation for litigation.

IV. Sources of Information

During the investigation, several sources of information were relied upon to fully understand the breadth of the situation. The sources of information consisted of a review of declarations, depositions, physical media devices, virtual (cloud-based) data, and personal interviews. The categories for each source of information are detailed below:

Declarations:

- B. Stein (12.8.20).pdf
- B. Stein Declaration (12.4.20).pdf
- J. Calise Declaration (12.4.20).pdf
- J. Stein Declaration (12.4.20).pdf
- J. Stein Declaration (12.10.20).pdf
- R. Manjoney Declaration (12.4.20).pdf

Depositions:

- B. Stein Deposition (3.8.19).pdf
- B. Stein Deposition (6.28.18).pdf
- J. Stein Deposition (7.1.19).pdf
- J. Stein Deposition (7.1.19).pdf

Physical Media Devices:

- Needle | Cuda's USB external hard drive
- Needle | Cuda's flash drive with loose emails
- Stein home computer forensic image

Virtual Data:

- Needle | Cuda's Dropbox account (Limited to Stein home computer files)
- FAA's SharePoint site

Personal Interviews (with dates):

- Reich & Truax, PLLC (Divorce counsel for Barry Stein)
 - ✓ Veronica Reich, attorney: 05-25-2021, 06-08-2021 and 06-17-2021
 - ✓ Dan Roberts, attorney: 06-08-2021 and 06-17-2021
 - ✓ Bernadette Iadorolo, assistant: 06-17-2021
 - ✓ Linda Cino, assistant: 06-17-2021
 - Needle | Cuda (Original divorce counsel for Jennifer Stein)
 - ✓ Melissa Needle, attorney: 06-17-2021, 08-11-2021
 - ✓ Jessica Calise, assistant: 06-03-2021, 06-17-2021 and 08-11-2021
 - ✓ Noelle LoPresti, assistant: 06-17-2021
 - ✓ Chris Lynch, IT: 08-19-2021, 08-26-2021
- * Present for all Needle | Cuda interviews - Michael Tripicco of Morrison Mahoney LLP

- Manjoney Technology Solutions (IT professional for Barry Stein/FAA)
 - ✓ Robert Manjoney: 06-17-2021
- Vista Computer Systems LLC (IT professional for Reich & Truax)
 - ✓ Edmund Humiston: 06-18-2021, 08-25-2021 and 08-27-2021
- Barry Stein: 04-27-2021
- Sylint Cyber Security, Forensics & eDiscovery (Sylint) (IT professional hired to forensically image Stein home computer)
 - ✓ John Jorgenson 04-29-2021
- Mandelbaum Salsburg P.C. (Counsel for FAA)
 - ✓ Steven Teppler: 06-29-2021
 - ✓ Ronen Yair: 06-29-2021

V. Timeline of Events

The acquisition and dissemination of the FAA patient and employee records has a timeline of events that can be traced from the source to the landing locations. Below are the key dates and subsequent actions by involved parties:

- **04-02-2018** – Jessica Calise (and Jennifer Stein) copied FAA patient and employee records (amongst other data) from the Stein home computer to a Needle | Cuda external USB hard drive. Subsequently, Jessica Calise copied the data to the firm’s server “K:\” drive and uploaded a copy of the data to the firm’s Dropbox account.
- **04-04-2019** – Jessica Calise sends an email to Veronica Reich that contains a link to the Needle | Cuda Dropbox site that provides access to the data that was copied from the Stein home computer.
- **04-07-2019** – Veronica Reich forwards the email from Jessica Calise to Daniel Roberts, Bernadette Iadorolo, Linda Cino and Barry Stein that contains the Needle Cuda Firm’s Dropbox link.
- **04-10-2019** – Bernadette Iadorolo is tasked with accessing the Needle | Cuda’s Dropbox link to manually create a written inventory of the contents of the site. Iadorolo identifies FAA patient and employee records and notifies Daniel Roberts.
- **Unknown date** – Bernadette Iadorolo downloads the data to the Reich & Truax server.

- **06-03-2019** – Robert Manjoney receives email from Bernadette Iadorolo that contains the Needle | Cuda Dropbox link.
- **06-11-2019** – Robert Manjoney notifies Barry Stein and Reich & Truax, PLLC about the lack of security with the Needle | Cuda Dropbox link.
- **08-02-2019** – Bernadette Iadorolo and Edmund Humiston create two encrypted flash drives with a copy of the FAA patient and employee records and ship those via FedEx to Ronen Yair.
- **08-02-2019** – Bernadette Iadorolo and Edmund Humiston create two flash drives with a copy of the FAA patient and employee records for storage in a locked cabinet at Reich & Truax. Humiston and Iadorolo then delete the data from the server.
- **09-30-2019** – John Jorgenson creates a forensic image of the Stein home computer per the direction of Steven Tepler.
- **10-18-2019** – Daniel Roberts sends an email to Steven Tepler that contains the Needle | Cuda Dropbox link.
- **12-04-2020** - Jessica Calise sends an email to Noelle Lo Presti with the Dropbox link to test the functionality of the newly added password protection on the account.

VI. Conclusions (Prior to 10-31-2021 Addendum)

During this investigation, all parties were aware their systems and networks were subject to onsite inspection by the forensic computer expert/special master. The purpose of the personal interviews was to understand each person's knowledge of the situation, the depth of involvement, and to gauge forthrightness and level of cooperation. The purpose of taking possession of physical devices and data stored in cloud-based accounts was to verify FAA patient and employee records were possessed outside of the Stein home computer and FAA SharePoint site.

SCI is confident that all parties were frank in their responses during the interview process, and as such, corroborated by the review of physical devices and cloud-based accounts. Therefore, the locations of FAA patient and employee records have been accounted for that violate Health Insurance Portability and Accountability Act (HIPAA) compliance. Those locations are as follows:

- ✓ On the “K:\” drive on a server located at Needle | Cuda
- ✓ On a USB external hard drive connected to a server at Needle | Cuda
- ✓ In a Wasabi cloud-based account belonging to the Needle | Cuda
- ✓ In a Wasabi cloud-based account (transferred via the ICXpress service) belonging to at Needle | Cuda
- ✓ In a Wasabi cloud-based account (transferred via the ICXpress service) belonging to ICEXpress
- ✓ In a Dropbox cloud-based account belonging to Needle | Cuda
- ✓ On an external hard drive in the possession of SCI belonging to the Needle | Cuda
- ✓ On two flash drives within the Reich Truax, PLLC firm
- ✓ In a Datto cloud-based account (transferred via a Datto Alto L3A2000 encryption appliance) belonging to the Reich & Truax, PLLC firm
- ✓ In a forensic image of the Stein home computer, possessed by Sylint Group
- ✓ In a forensic image of the Stein home computer (two copies), possessed by SCI
- ✓ In a forensic image of the FAA SharePoint collection possessed by SCI
- ✓ In loose file format of the FAA SharePoint collection possessed by SCI
- ✓ In loose file format of the Needle | Cuda Dropbox collection possessed by SCI

A copy of the FAA data that previously existed on the Reich & Truax, PLLC’s server was deleted remotely by Edmund Humiston with the assistance of Bernadette Iadorolo on 08-02-2019.

A copy of the FAA data that previously existed in a Carbonite cloud-based account belonging to Needle | Cuda was eliminated on 08-09-2020 after the account was closed and Carbonite’s 30-day retention policy expired.

Lastly, I’ve determined the following persons received an email that contained Needle | Cuda’s Dropbox link and would have illegitimate access to the FAA patient and employee records if downloaded:

- ✓ Veronica Reich
- ✓ Daniel Roberts
- ✓ Bernadette Iadorolo
- ✓ Linda Cino
- ✓ Jessica Calise
- ✓ Noelle Lo Presti
- ✓ Robert Manjoney

As of 12-04-2020 access to the FAA patient and employee records via the Needle | Cuda Dropbox location was prohibited due to password protection being enabled on that date. Therefore, the original email with the link sent to various parties will no longer provide access. SCI has confirmed that access to the records via the link in the original email is no longer functioning. There is no evidence anyone has the password to the site except for Jessica Calise and SCI. Therefore, forensic access to the full email accounts of persons that previously received the email containing the Dropbox link and a subsequent manual targeted deletion of those emails from their accounts is not necessary.

VII. Recommendations for Remediation (see Addendum page 20 for updates)

SCI is satisfied the ***Conclusions*** section of this report describes the only locations the FAA patient and employee records currently exist and fall outside of HIPAA compliance. SCI is requesting the appropriate relief from the Superior Court to execute the permanent deletion (or preservation for ongoing litigation) of the confidential patient and employee information at the following locations listed below and via the methods noted:

- ✓ On the “K:\” drive on a server located at the Needle | Cuda office
 - Remote computer access with targeted deletion and wiping by SCI.
- ✓ On a USB external hard drive connected to a server at the Needle | Cuda office
 - Remote computer access with targeted deletion and wiping by SCI.
- ✓ In a Wasabi cloud-based account with a server-level backup scheme belonging to Needle | Cuda
 - No manual deletion is necessary due to the automatic deletion from the backups when synced with the K:\ drive (noted above). These server-level backups last for three weeks and have a first-in/first-out deletion function.
- ✓ In a Wasabi cloud-based account with a file-level backup scheme (transferred via the ICXpress service) belonging to Needle | Cuda
 - There are 3-years’ worth of backups that can undergo manual targeted deletion performed by ICEXpress.
- ✓ In a Wasabi cloud-based account with a file-level backup scheme (transferred via the ICXpress service) belonging to ICEXpress
 - There are 3-years’ worth of backups that can undergo manual targeted deletion performed by ICEXpress.
- ✓ In a Dropbox cloud-based account belonging to Needle | Cuda
 - Remote access with manual targeted deletion by SCI.
- ✓ On an external hard drive in the possession of SCI belonging to Needle | Cuda
 - Manual targeted deletion with wiping by SCI.
- ✓ On two flash drives within the Reich Truax, PLLC firm
 - Remote computer access with manual targeted deletion and wiping by SCI.
- ✓ In a Datto cloud-based account (transferred via a Datto Alto L3A2000 *encryption appliance*) belonging to the Reich & Truax, PLLC firm

- Total wipe of the appliance and deletion of the Datto account by Edmund Humiston with SCI observing **or** enter into a formal agreement. A court order that future restorations of backups, that occurred during April-August 2019, will require notifications to counsels for FAA of said restoration(s) accompanied by immediate targeted manual deletion of the FAA patient and employee records from the newly restored data. NOTE - It is not technically possible to perform manual targeted deletions from the Datta cloud-based location of specific full backups or portions thereof. Therefore, the firm will lose a significant amount of previously backed up data if ordered to wipe the appliance and delete the account.
- ✓ In a forensic image of the Stein home computer, possessed by Sylint
 - Surrender of all physical storage mediums containing copies of the forensic image (i.e., hard drives in Sylint's evidence vault or stored virtual data) by sending the storage mediums to SCI for evidence vault preservation **or** deletion from storage mediums/virtual data.
- ✓ In a forensic image of the Stein home computer (two copies), possessed by SCI
 - Preservation in SCI's evidence repository **or** physical destruction of the original hard drive acquired from Sylint and manual targeted deletion of the forensic image from SCI's working forensic hard drive.
- ✓ In a forensic image of the FAA SharePoint collection possessed by SCI
 - Preservation in SCI's evidence repository **or** deletion of the forensic image from SCI's working forensic hard drive by SCI.
- ✓ In loose file format of the FAA SharePoint collection possessed by SCI
 - Preservation in SCI's evidence repository **or** targeted deletion from SCI's working forensic hard drive.
- ✓ In loose file format of the Needle | Cuda Dropbox data collection possessed by SCI
 - Preservation in SCI's evidence repository **or** targeted deletion from SCI's working forensic hard drive

Lastly, SCI was advised that possession of the FAA patient and employee records are lawfully permitted by the law firms Mandelbaum Salsburg P.C., Cohen and Wolf, P.C., and Frost | Bussert LLC due to their interest/involvement in the litigation and no authorization for relief from the court is being requested for those firms.

Via this report, SCI is requesting the court to provide final instructions for remediation of the FAA patient and employee records where there is a choice between preservation of evidence at SCI (due to litigation) or permanent deletion.



John R. Clingerman, CFCE

The findings and conclusions contained within this report are based upon information and materials made available to Special Counsel by the Parties. Special Counsel reserves the right to reassess any of the above based upon additional information or materials that might be presented to it, or to examine in greater depth or detail should the Parties or court so direct. The contents of this document are privileged and confidential.

CONFIDENTIAL

Addendum

After submission of the original report (08-27-2021) and a revised version (09-01-2021) that contained corrections of three names, all parties were advised that an inspection would be performed on computers, external devices and web-based accounts for the Needle | Cuda and Reich & Truax firms. The purpose of the inspection would be to verify information gathered during the interviews as well as determine if there were additional sources of FAA patient and employee records present. SCI advised all parties to expect an addendum to the revised report after the inspections and analyses were complete. This addendum contains updates to two Timeline of Events, the results of the inspections, additional interviews, subsequent analyses, and a final list of devices with suggested remediation steps.

On 09-22-2021, SCI performed a telephone conference call and a remote access computer session with Chris Lynch of Needle | Cuda with the assistance Herb Marcucilli, a private IT consultant who were both physically in place at the Needle | Cuda firm.

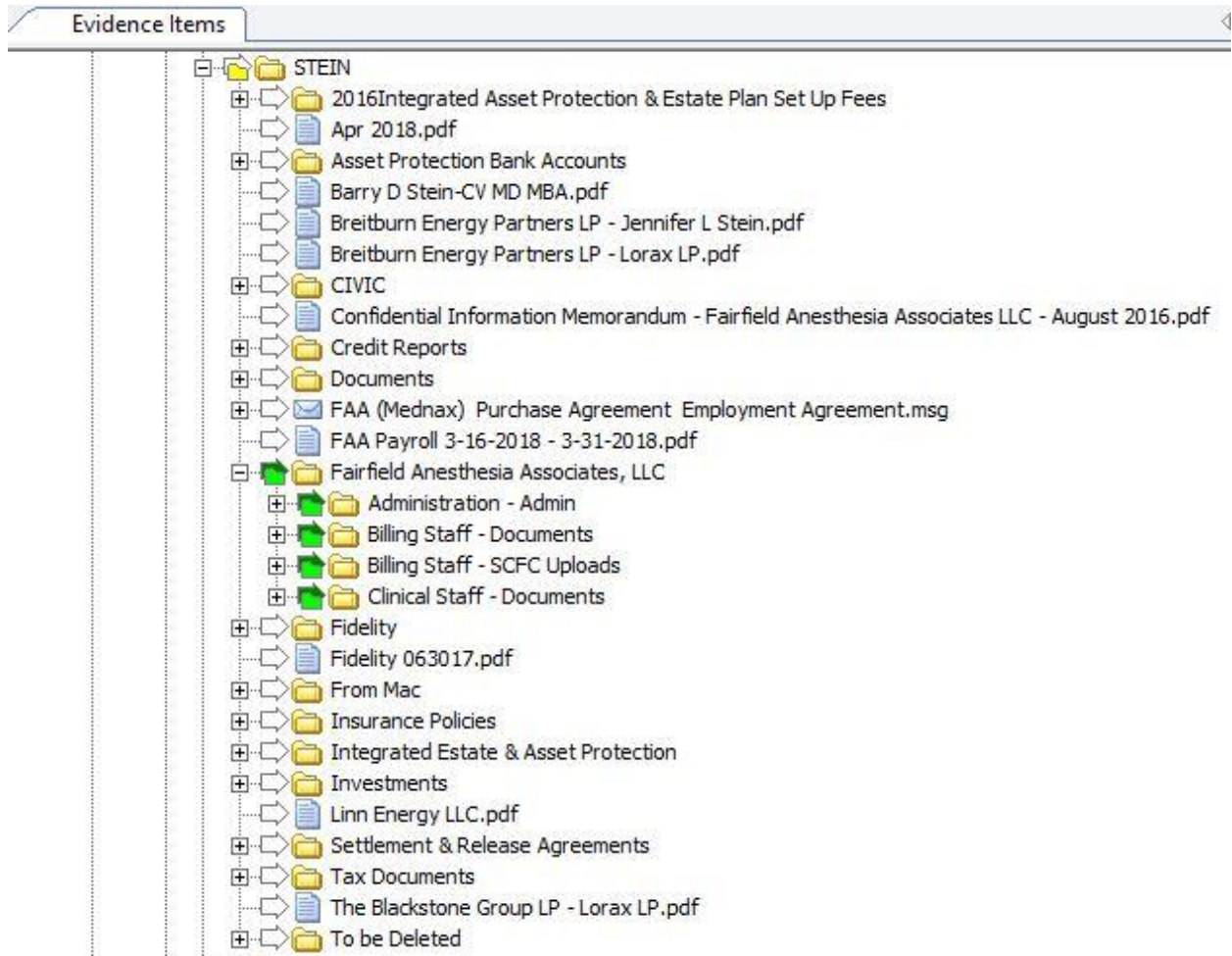
The list below represents the devices in the Needle | Cuda firm that could potentially contain FAA data:

- Hewlett Packard Enterprise (HP) physical server s/n: MXQ00207ND named NCLO-SVR-DC01, contained:
 - ✓ K:\ drive – Mapped network drive used for storage of client data
- Virtual server named NCLO-HYPERV-01, contains:
 - ✓ ICXBackup (encrypted server backup)
 - ✓ USB external hard drive (encrypted server backup)
- Dell Precision T3610 desktop s/t: 1X22M02, known as “Reception” used by Noelle LoPresti with a user profile “Noelle”
- Lenovo Think Center M83 desktop s/n: 1S10AHS01700MJ01FYL7, used by Jessica Calise with user profile “jessica.needlelawoffice”

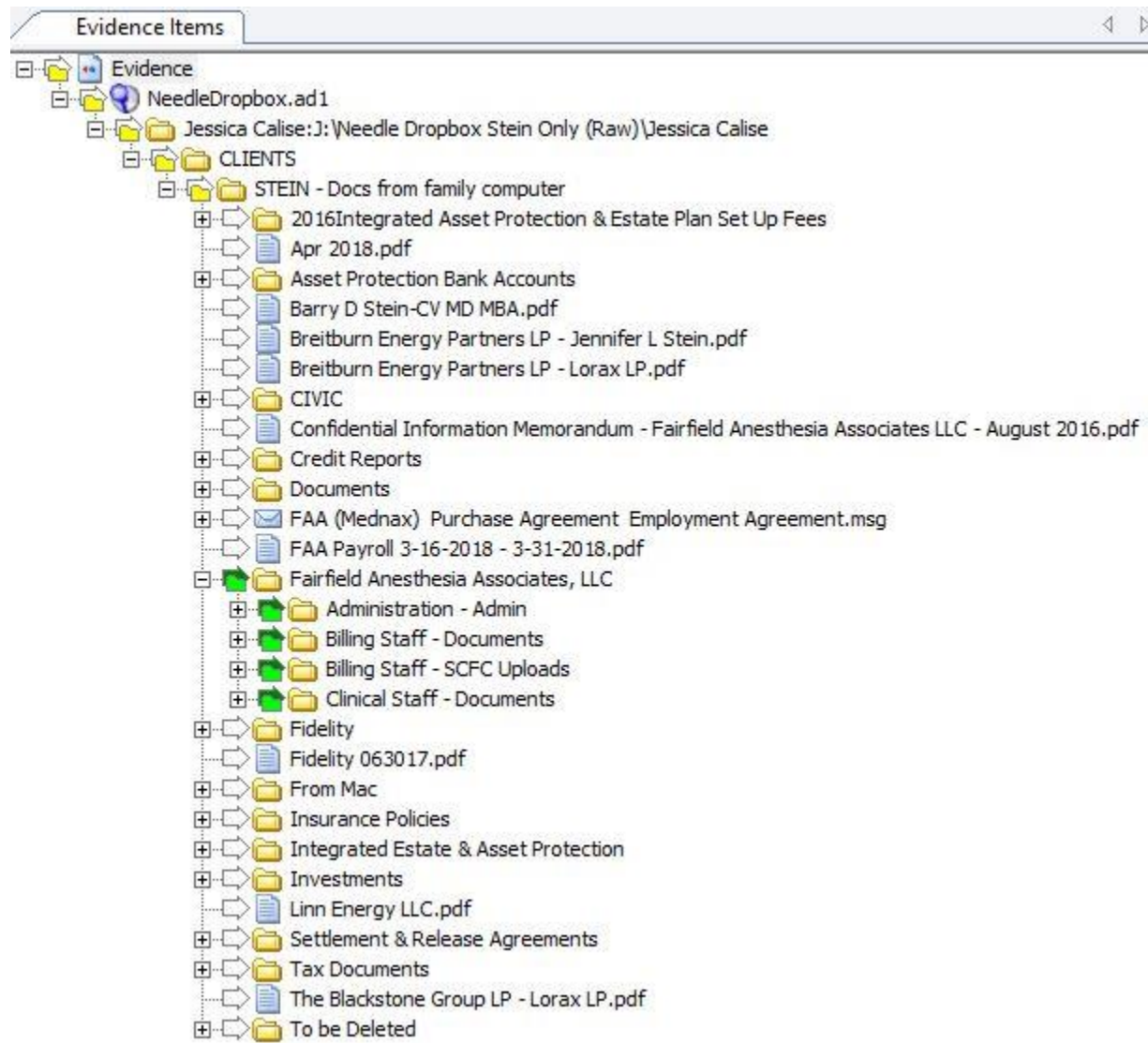
The inspections were performed on the HP server, LoPresti desktop, and Calise desktop but not on the ICExpress or USB external hard drive due to their encrypted contents. The inspection consisted of a manual visual review of folders and files that included but were not limited the folders Desktop, Documents, Downloads, OneDrive, Dropbox, mapped network locations (i.e., LoPresti and Calise computers direct access to the HP server), and by the execution of unique search terms via File Explorer. In summary, there were many files related to the Stein matrimonial case present on the server, Calise and LoPresti computers, but the FAA patient and employee records were located only on the K:\ drive of the HP server.

A forensic image was created of the folder named “Docs From Family Computer” and its subfolders and files located on the server’s K:\ drive and was sent to SCI for analysis.

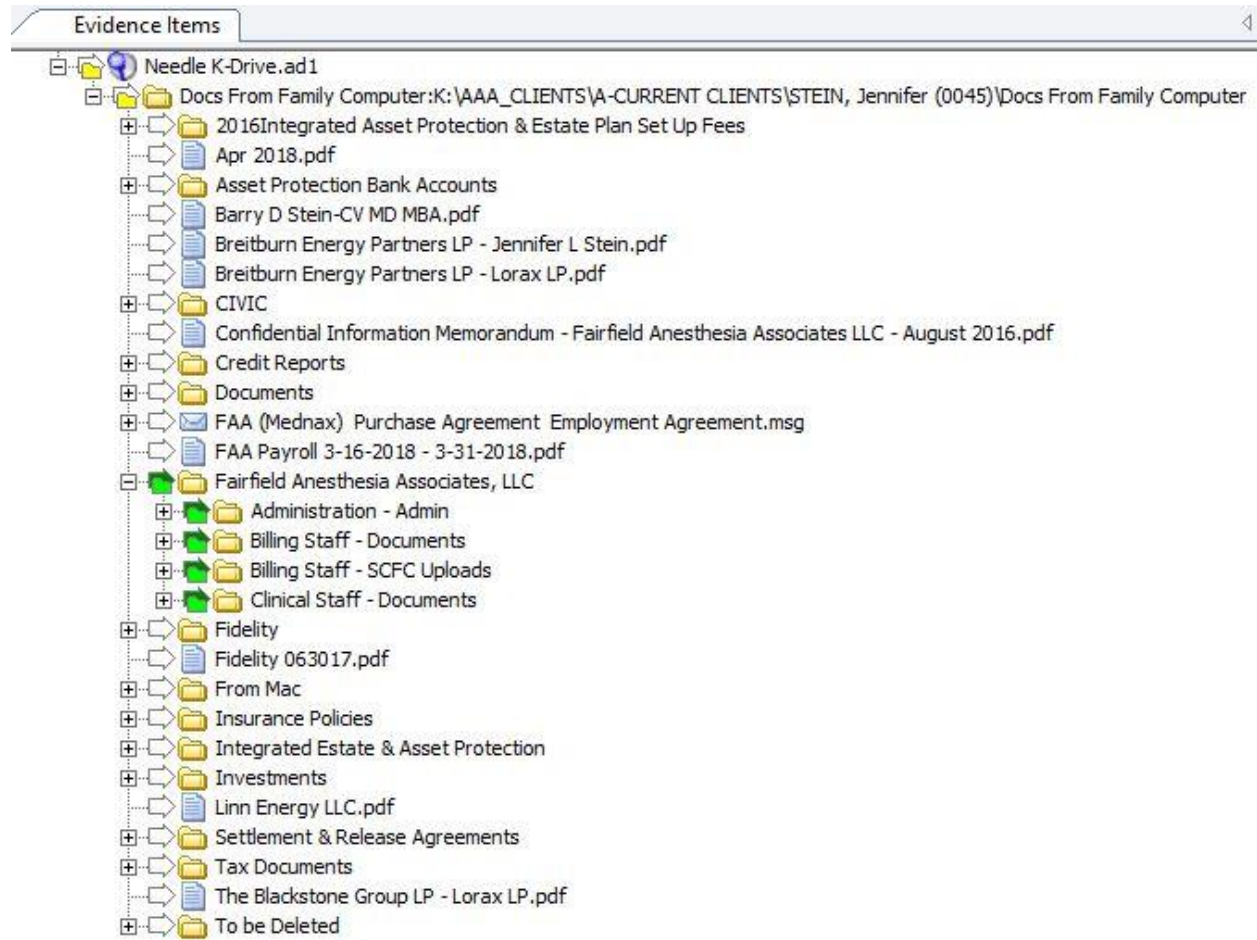
Below is a screenshot of the FAA data set on the **Needle | Cuda external hard drive**. Note the green icons drawing attention to the FAA data. The content of the FAA patient and employee records consisted of 2,572 folders and 13,998 files totaling 8.37GB in size.



Below is a screenshot of the FAA patient and employee and records in the **Needle | Cuda Dropbox**. Note the green icons drawing attention to the FAA patient end employee records. The content of the FAA patient and employee records consisted of 2,563 folders and 13,636 files totaling 7.93GB in size.

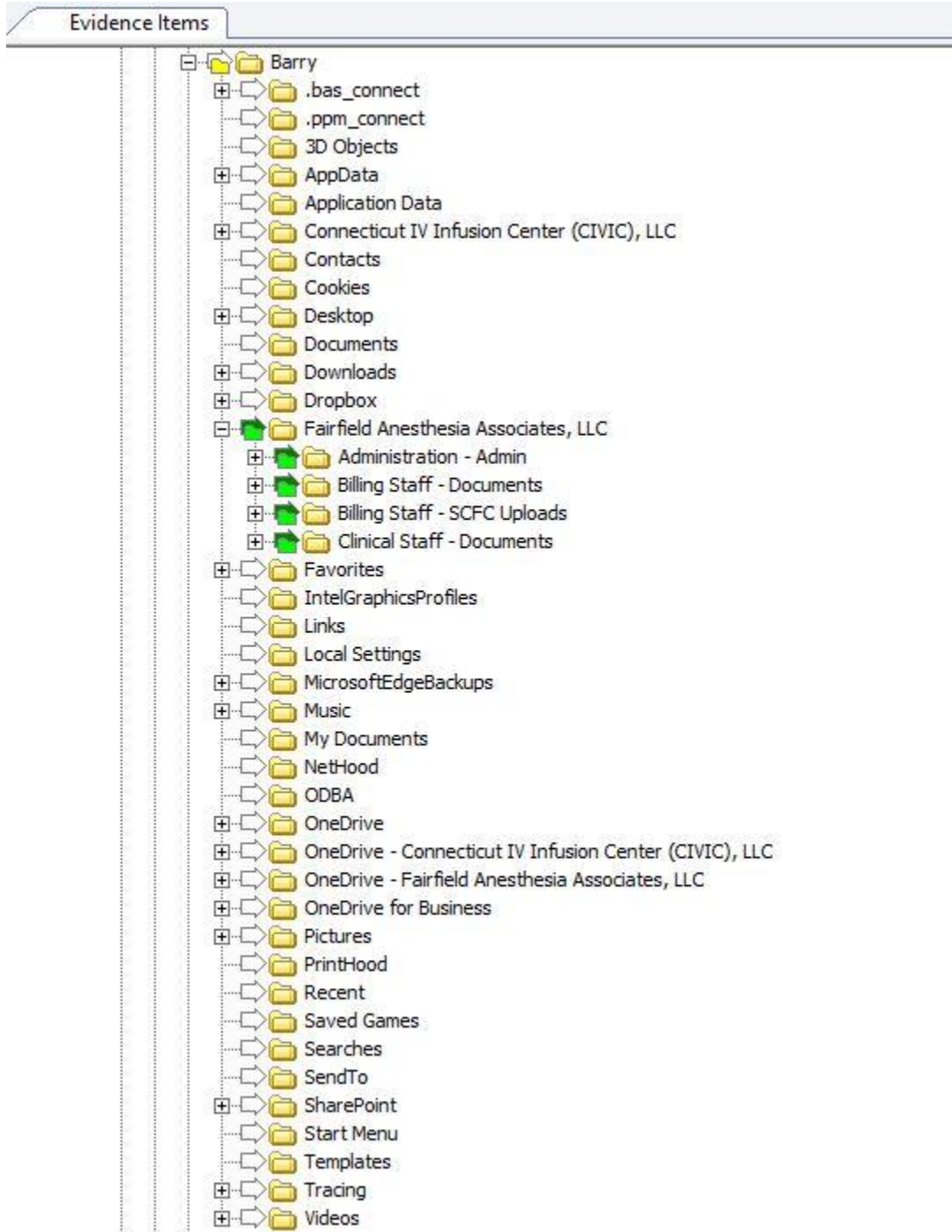


Below is a screenshot of the FAA patient and employee records set in the **Needle | Cuda server's K:\ drive**. Note the green icons drawing attention to the FAA data. The content of the FAA patient and employee records consisted of 2,572 folders and 4,431 files totaling 4.85GB in size.



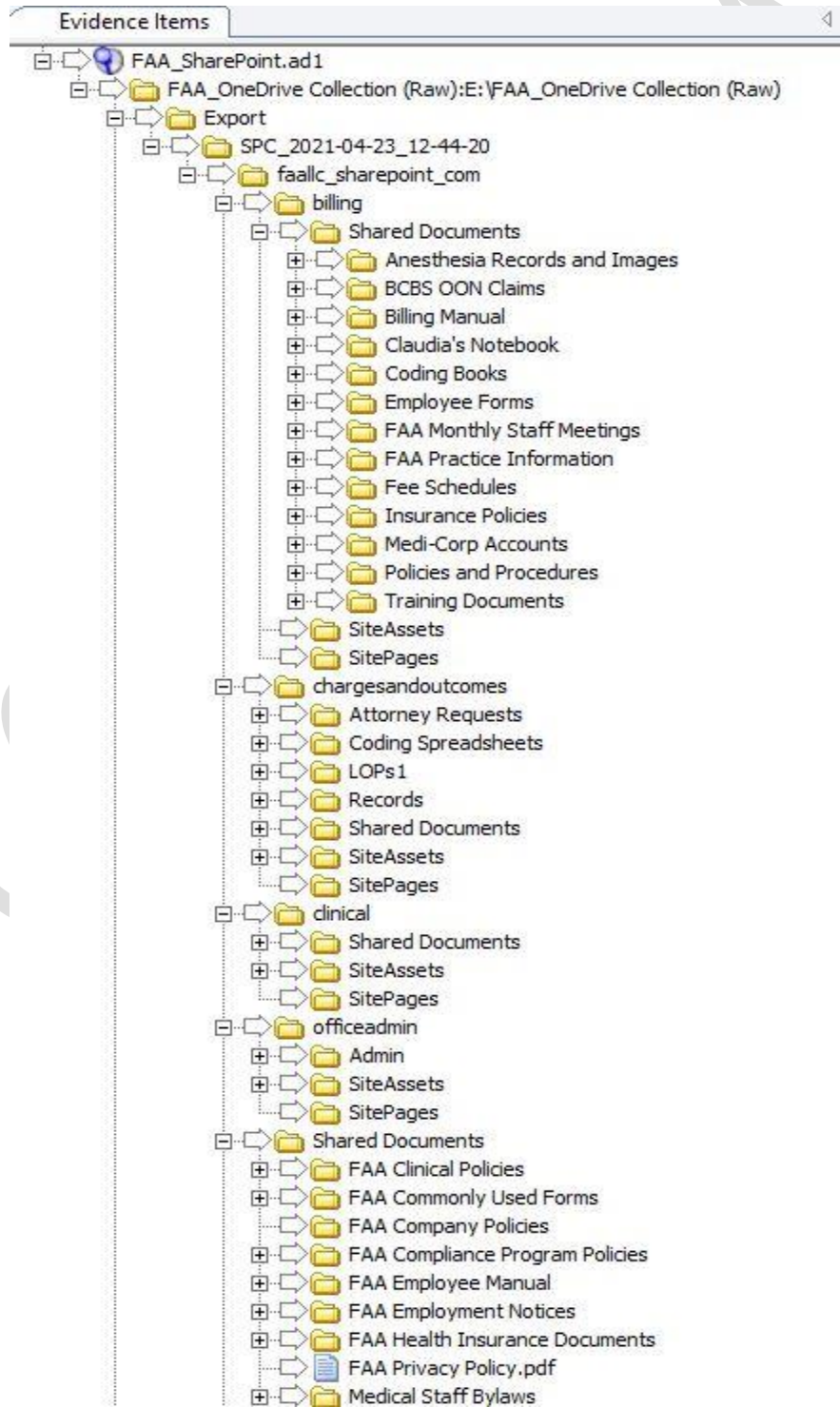
Comparisons were then performed of the FAA patient and employee records located on the Stein home computer against the devices in control of Needle | Cuda, those being the external hard drive, the Dropbox account and the K:\ drive.

Below is a screenshot of the “Barry” user profile in the **Stein home computer**. Note the green icons drawing attention to the FAA patient and employee records. The content of the FAA patient and employee records consisted of 3,472 folders and 18,261 files totaling 9.04GB in size. NOTE – On 09-30-2019, Jorgenson collected the data depicted below. That date was almost 1.5 years after the 04-02-2018 date Calise copied the FAA patient and employee records from the computer. During that time span, at least 900+ folders and 4200+ files were added to the data set on the home computer.



The Stein home computer contained five additional user profiles, as follows: “BarryDSteinM_yy7sjg9”, “BarryDSteinMDMBA”, “FAAAdministrator”, “ITAdministrator”, and “jlste_000”. None of these additional five user profiles contained the FAA patient and employee records that mimic the FAA patient and employee records in the “Barry” user profile or the FAA patient and employee records in control of Needle | Cuda.

Moreover, vastly different was the organization of the FAA data seen in the **FAA Sharepoint** account depicted in the screenshot below. None of the data below mimics the layout of the FAA patient and employee records in the Stein home computer or in control of Needle | Cuda.



In summary, the FAA patient end employee records in control of Needle | Cuda originated directly from the Stein home computer and not directly from the FAA SharePoint site. Additionally, metrics show that some of the data did not transfer each time the data was copied at Needle | Cuda to other locations within Needle | Cuda as evidenced by folder and file counts. A summary of metrics for the FAA data in control of Needle | Cuda are as follows:

- USB External hard drive – 2572 folders, 13,998 files – 8.37GB in size
- Dropbox account – 2,563 folders, 13,636 files – 7.93GB in size
- Server K:\ drive – 2,572 folders, 4,431 files – 4.85GB in size

Lastly, also on 09-22-2021 Chris Lynch and SCI conducted a telephone conference call with Peter Tomlinson, a network administrator for Wasabi/ICXpress, the server backup service utilized by Needle | Cuda. Tomlinson stated the daily server-level backups would expire after two weeks, not three weeks as previously noted (see page 10). Additionally, Tomlinson will be capable of performing targeted deletions of file-level backups as well as encrypted backups created via ICXpress. The only requirement is to provide the folder pathing of “Fairfield Anesthesia Associates, LLC” as the upper-level folder name to perform targeted deletions from the Wasabi and ICXpress systems.

On 09-22-2021, SCI performed a telephone conference call and a remote access computer session with Edmund Humiston of Vista Computer Systems and Bernadette Iadorolo of Reich & Truax.

The list below represents the devices in the Reich & Truax firm that could potentially contain FAA patient and employee records:

- HP ProLiant ML10 Generation 10 server (s/n: 2M290701HZ), contains:
 - ✓ G:\ Veronica – Mapped network drive with client data
- HP Compaq Elite 8300 desktop (s/n: 2UA3020F9Z 2021) with user profiles “bernadette” and “Bernadette.laxwin7” (Iadorolo’s previously used computer)
- HP EliteDesk 900 desktop (s/n: MXL925546V), with user profile “Bernadette” (placed into service 07-28-2021)
- Western Digital Passport external hard drive (s/n: 575842314141343543313536), contains:
 - ✓ Server BU (stands for server backup)
- 1 - Verbatim Store-N-Go flash drive (s/n: 4290A015E5D9D80061D1)
- 2 - Verbatim Store-N-Go flash drive (s/n: 83D270B615B877E5BB4E)
- 3 - Verbatim Store-N-Go flash drive (s/n: C0005752E51C4C65)

The inspections were performed on the HP server, both of Iadorolo's desktops, the Western Digital external hard drive and the three Verbatim flash drives. The inspections consisted of a manual visual review of folders and files that included but were not limited to the folders Desktop, Documents, Downloads, OneDrive, Dropbox, mapped network locations (i.e., Iadorolo had direct access to the HP server), and by the execution of unique search terms via File Explorer. Note, computer users within the firm save all data to the server, not their local computers. In summary, there were many files related to the Stein matrimonial case present on the server, but the FAA patient and employee records were not present. The FAA patient and employee records and notations were present on all three Verbatim flash drives. SCI then created forensic images of the three Verbatim flash drives for analysis.

Although all three Verbatim flash drives contained some level of FAA patient and employee records, none contained an identical cataloging/folder system as the FAA patient and employee records seen in the Stein home computer or the Needle | Cuda devices. Therefore, a discerning targeted deletion approach will be required to eliminate information about patients (i.e., folder names, letters to, invoices, medical records, etc.) from the Verbatim flash drives. Note, no screenshots are present in this addendum due to the confidential nature of the patients' names and records.

During the telephone conference call with SCI, Humiston corrected the information he previously supplied SCI as it related to the Datto Alto L3A2000 encryption appliance. He further explained the firm's server backup system prior to December 2019 was an external hard drive connected to the server and utilizing a free software called "Karen's Replicator." In December of 2019, the firm started using the Datto appliance and cloud storage system. This system was not in use during April-August of 2019 as previously cited. Therefore, considering the receipt of the FAA patient and employee records occurred at Reich & Truax before the Datto appliance went into service, there will be no FAA patient and employee records on the appliance or in the cloud storage. Therefore, disregard previous comments regarding remediation of data on the Datto system and its cloud storage location as mentioned in the original report (seen on pages 10 and 11).

Updated Recommendations for Remediation

Maintain the original list of recommendations and processes as noted on pages 10 and 11 of the report with the following updates:

- ✓ **Disregard** all references to the Datto Alto L3A2000 encryption appliance and cloud backup belonging to Reich & Truax.
- ✓ **Add** one additional Verbatim flash drive, making a total of three in the possession of Reich & Truax.

EXHIBIT A

John R. Clingerman

Manager, Digital & Cyber Forensic Services
John.clingerman@specialcounsel.com

BIOGRAPHY

John has been with Special Counsel / EQ since its purchase of D4, LLC in September of 2017 and is currently a Manager within the Digital & Cyber Forensic Services. Prior to that, John was with D4, LLC and a Vice President and member of the company's Forensic Services Group since 2007. John's responsibilities are varied and include project management of digital forensic and data collection projects, overseeing laboratory operations, personnel and equipment in the Rochester, NY and Tampa, FL offices, and personally assisting on projects. John has conducted several digital evidence collections and computer forensic examinations and provides peer review to other examiners.

John came to D4 after retiring from law enforcement with over 24 years of service, the last 14 years holding the rank of Police Investigator. During his career, he held several positions including Patrolman, Youth Officer/D.A.R.E. Instructor, Evidence Technician, Firearms Instructor, and Narcotics Task Force Supervisor. He has investigated all types of major felony crimes including murder, rape, robbery, burglary and also many types of computer related criminal activities. He has testified hundreds of times in all levels of criminal court from local to federal. In November 2006, he was featured in the National White Collar Crime Center's quarterly issued magazine for uncovering a major international identity theft ring. He has earned many citations during his career including Officer of the Year and two Life Saving Awards.

John's computer forensic trainings have been with the National White Collar Crime Center, International Association of Computer Investigative Specialists (IACIS), Guidance Software, Access Data Corporation and Sumuri Forensics. He is a Certified Forensic Computer Examiner (CFCE), a Certified Cellebrite UFED Mobile Device Examiner, and a Certified Electronic Evidence Collection Specialist (CEECS). He has taught computer forensics at a local community college as well as coached others in the law enforcement community with the CFCE process. John is also a licensed Private Investigator in New York State, Florida and Texas.

PROFESSIONAL EXPERIENCE

Special Counsel, Tampa, FL

Manager, Digital & Cyber Forensic Services, July 2019 to present

- Managing the forensic laboratory environment in Tampa, FL
- Project management of data collections and forensic examination engagements
- Conducting forensic examinations
- Perform data collections in the field
- Peer review
- Assist management when hiring personnel for the Digital & Cyber Forensic Services group at large
- Provide court room testimony
- Public speaking engagements

Special Counsel, Rochester, NY

Manager, Digital & Cyber Forensic Services, January 2019 to July 2019

- Managing the forensic laboratory environment and personnel within the Rochester, NY office
- Project management of data collections and forensic examination engagements
- Conducting forensic examinations
- Peer review
- Assist management when hiring personnel for the Digital & Cyber Forensic Services group at large
- Provide court room testimony
- Public speaking engagements

D4, LLC, Rochester, New York

Vice President Forensic Services, January 2010 to January 2019

- Project management of all data collections and forensic examination engagements
- Invoicing
- Hiring personnel
- Managing the forensic laboratory environment and all levels of personnel and activities within
- Conducting forensic examinations
- Peer review
- Provide court room testimony
- Public speaking engagements

Data Forensics and Collections Manager, September 2007 to January 2010

- Managing the forensic laboratory environment to include data technicians and evidence clerk
- Overseeing the evidence intake and disposition process
- Conducting forensic examinations
- Assisting project management with assigning resources
- Provide court room testimony
- Public speaking engagements

Computer Forensic Analyst, February 2007 to September 2007

- Conducted forensic examinations on computers and cell phones

Town of Macedon, NY Police Department, Macedon, NY

Police Investigator, January 2011 to 2015

- Investigate felony crimes that are electronic in nature and perform mobile device forensic examinations for the narcotics task force in Wayne County, NY

Finger Lakes Community College, Canandaigua, New York

Adjunct Instructor, January 2006 to May 2007

- Instructed college students in the topic of Computer Forensics

Newark, NY Police Department, Newark, New York

Police Investigator, October 1993 to September 2007

- Investigated all felony crimes, which include murder, rape, robbery, burglary, narcotics trafficking, and crimes committed with computers

Supervisor Wayne County Narcotics Enforcement Team, February 2006 to September 2007

- Coordinated all police personnel from various county departments and all activities during undercover narcotics investigations and search warrant executions

Youth Officer/D.A.R.E. Officer, June 1989 to October 1993

- Investigated all crimes committed by persons 15 years of age and younger, provided educational and public speaking engagements for the department

Patrolman, March 1983 to June 1989

- Patrolled the village in marked police car, first responder to all incidents, investigated citizen complaints and traffic accidents

CERTIFICATIONS

- Certified Forensic Computer Examiner (CFCE) – Continuously recertified since 2008
- Certified Electronic Evidence Collection Specialist (CEECS)
- Certified Cellebrite UFED Mobile Device Examiner
- Private Investigator – Licensed in New York State, Florida and Texas
- New York State Certified Police Officer – Finger Lakes Law Enforcement Academy

EDUCATION

B.S. in Computer Forensics and Digital Investigations – May 2013

Champlain College, Burlington, VT

- GPA 4.0 – Graduated Summa Cum Laude
- Member of Honor Society Alpha Sigma Lambda

A.A.S. Degree in Information Technology - May 2010

Finger Lakes Community College, Canandaigua, NY

A.A.S. Degree in Criminal Justice May 1982

Finger Lakes Community College, Canandaigua, NY

EXPERT TESTIMONY, AFFIDAVITS AND DECLARATIONS

During a law enforcement career spanning over 24 years, testimony has been given hundreds of times in all levels of courts (local, state and federal) during various types of hearings and at trial on a multitude of criminal matters which include: murder, rape, robbery, burglary, major narcotics trafficking, and also many types of computer related criminal activities (child pornography, identify theft, and grand larceny).

During a corporate career spanning over eleven years, testimony has been given:

- For Civil Plaintiff – August 2021 at deposition for the Matter Gregory M. Hall Trust Agreement, Court File No. 2018-383,234-TV, Oakland County Probate Court, Michigan
- For Plaintiff – December 2020 at deposition (final half) for Commodity Solutions Inc. vs. Abner, et al., Case No. CI 16-3122, in the District Court Platte County, Nebraska
- For Plaintiff – October 2020 at deposition (first half) for Commodity Solutions Inc. vs. Abner, et al., Case No. CI 16-3122, in the District Court Platte County, Nebraska
- For Plaintiff – July 2020 at hearing for HBW vs. Gentry, et al., Civil Action No. 1:20-cv-00395-RBJ, in the United States District Court for the District of Colorado
- For Plaintiff – July 2020 at deposition for HBW vs. Gentry, et al., Civil Action No. 1:20-cv-00395-RBJ, in the United States District Court for the District of Colorado
- For Plaintiff – April 2019 at deposition for Gene Stamper and Alicia Stamper vs. Northern Arizona Health Care Corporation, No. CV2016-00259, Superior Court, Coconino County, Arizona
- For Criminal Prosecution – May 2018 at trial for People of the State New York vs. Robert DePalo, Supreme Court, Criminal Term Part 59, Indictment # 04150-2015.
- For Civil Defendant – February 2017 at deposition for Office Depot, Inc. et al vs. Roberts, Case No. 1:2016cv04234 in the New York Southern District Court.
- For Civil Plaintiff – April 2016 at hearing In The Matter of the Estate of William R. Nunz, File No. 2012-4075 in the Surrogate's Court of Erie County, Buffalo, NY.
- For Civil Defendant – October 2013 at arbitration hearing for Kevin Wailes v. Tel-Networks, USA, LLC, JAMS Arbitration No. 1425013444 in Manhattan, NY.
- For Civil Defendant – September 2013 at trial for Michael Weidner vs. Lisa Six Weidner, Index No. 9621/2012 in the State Supreme Court, Monroe County, NY.
- For Civil Plaintiff - June 2012 at second deposition for American Builders & Contractors Supply Co., Inc. vs. Roofers Mart, Inc., Bernard S. Miller Jr., Michael L. Burger, Lucas Y. Abbott, Mark E. Lineberry, Daniel Woodall, Steven G. Declue, and John E. Slattery, Case No. 1:11-cv-00019 CEJ in the United States District Court for the Eastern District of Missouri
- For Civil Defendant – May 2012 at deposition for Juan and Ramona Medina vs. Pile Trucking, Inc., Case No. CV-11-06329 GHK in the United States District Court for the Central District of California Western Division
- For Civil Plaintiff - September 2011 at first deposition for American Builders & Contractors Supply Co., Inc. vs. Roofers Mart, Inc., Bernard S. Miller Jr., Michael L. Burger, Lucas Y. Abbott, Mark E. Lineberry, Daniel Woodall, Steven G. Declue, and John E. Slattery, Case No. 1:11-cv-00019 CEJ in the United States District Court for the Eastern District of Missouri Southeastern Division
- For Civil Defendant - July 2010 at trial for Haute Couture vs. Continental Casualty Company, Case No. 4:09-cv-809 JLH in the U.S. District Court, Eastern District of Arkansas, Western Division
- For Criminal Prosecution - October 2008 at Grand Jury New York County, NY for State of NY vs. Testwell, Inc.
- Generated dozens of affidavits that were subsequently submitted to various federal district courts

TRAINING

- Cyber Incident Forensic Response – IACIS, April/May 2021
- Best Practices in MAC Forensics, by Sumuri Forensics – IACIS, May 2018
- Windows Forensic Examiner Training – IACIS, May 2016
- Mobile Phone Forensic Examiner Training – IACIS, May 2015
- Certified Cellebrite UFED Physical Examiner Course – Sumuri Forensics, December 2012
- Macintosh Forensics Level 2 – Sumuri Forensics, July 2012
- Macintosh Forensics Level 1 – Sumuri Forensics, March 2012
- Universal Forensic Extraction Device (UFED) Mobile Device Examiner – Sumuri Forensics, August 2011
- Staff Member at Basic Computer Forensics Examiner (BCFE) Training – IACIS, May 2011
- Access Data Mobile Phone Examiner - Access Data Corp, November 2010
- Staff Member at Basic Computer Forensics Examiner (BCFE) Training – IACIS, May 2010
- EnCase II, Guidance Software, June 2009
- Advanced Microsoft Office Document Examination – IACIS, May 2009
- Advanced Windows Forensic Analysis – IACIS, April 2009
- Forensic ToolKit 2.0 – IACIS, May 2008
- Blackbag Technologies Macintosh Forensics – IACIS, May 2008
- Windows Forensics – Access Data, November 2007
- Certified Forensic Computer Examiner (CFCE) Basic Training – IACIS, April 2007
- Forensic ToolKit Boot Camp – Access Data, March 2007
- Advanced Data Recovery & Analysis – ILook, National White Collar Crime Center, May 2006
- Intermediate Data Recovery & Analysis – National White Collar Crime Center, April 2006
- Basic Data Recovery & Analysis – National White Collar Crime Center, February 2006
- Advanced Internet Search for Investigators – Monroe Community College, July 2004
- Computer Technology & Investigations – Monroe Community College, February 2004
- 1st Responders Seizure of Computers & Electronic Evidence – Division of Criminal Justice Services, May 2003
- Internet Train the Trainer – Bureau of Justice Assistance, October 1999
- New York State Juvenile Specialist, April 1994
- Firearms Instructor, October 1993
- Interview & Interrogation, November 1990
- General Topics Police Instructor, November 1989
- D.A.R.E. (Drug Abuse Resistance Education) Officer, October 1989
- Evidence Technician, March 1987

ARTICLES AND SPEAKING ENGAGEMENTS

- Independent Insurance Agents & Brokers of NY, Social Media Panel Discussion CLE, June 2015
- Western NY Paralegal Association, Best Practices for Social Media Collections and Investigations Part 1, April 2012
- Western NY Paralegal Association, Best Practices for Social Media Collections and Investigations Part 2, July 2012
- Presenter at Champlain College DFIR Online Case Study web-based presentation, February 2012
- Genesee County Bar Association Social Media Investigations (CLE), Buffalo, NY November 2011
- Presenter at Genesee County Bar Association Social Media Investigations (CLE), Buffalo, NY November 2011

- Presenter at Legal Med's Social Media Investigations, Buffalo, NY September 2011
- Presenter at Erie County Bar Association's "Facebook *Still* Got You All A- Twitter?" (CLE), Buffalo, NY March 2011
- Presenter at Association of Legal Administrators, Rochester, NY April 21, 2010
- Presenter at Erie County Bar Association, "Facebook Got You All A- Twitter?" (CLE), Buffalo, NY, March 2010
- Presenter at Western NY Certified Fraud Examiner's Meeting, SUNY Brockport, Brockport, NY, December 2009
- Presenter at Career Day, Lyons High School, Lyons, NY, October 2009
- Presenter at "Document Retention and Destruction" seminar in Rochester, NY, January 21, 2009
- Presenter at "Document Retention and Destruction" seminar in Buffalo, NY, January 13, 2009
- Presenter at Career Day, Corning Community College, Corning, NY, October 2008
- Presenter on Computer Forensics at Finger Lakes Community College in Canandaigua, NY, April 2008
- Expert Witness in Mock Rule 26-f Conference, Erie County Bar CLE, January 11, 2008
- "Best Practices on Preservation and Collection" presentation at Erie County Bar CLE, January 11, 2008
- Expert Witness in Mock Rule 26-f Conference, Trials Tactics & Technology Conference, New York, NY, November 2007

PROFESSIONAL ORGANIZATIONS

- Member of International Association of Computer Investigative Specialists (IACIS)
 - ~Past Member of Communications Committee
 - ~Past Staff Member at the Basic Computer Forensic Examiner Training
 - ~Past Website Administrator
 - ~Past CFCE process coach/mentor for law enforcement officers
- Member of High Technology Crime Investigation Association (HTCIA)
- Member of InfraGard
- Member of Williamson Flying Club – October 2012 to present
 - ~ Private Pilot License – June 2014
 - ~ Member Board of Directors - February 2015 to February 2018
 - ~ Member of Annual Pancake Breakfast Committee and Ticket Chairperson – May 2015 to 2019
 - ~Chairperson of Membership and Activities Committees – February 2016 to February 2018
- Member of Newark Elks Lodge #1249
 - ~Past Club Officer holding Tiler Position
- Past Member of Newark Park Presbyterian Church
 - ~Past Session Member
- Past Member of Newark, NY Rotary Club
 - ~Member of Rotary Group Study Exchange shadowing Argentine Federal Police, May 1999
 - ~Past Member Board of Directors 2002 to 2007
 - ~Past Website Admin
 - ~Past Youth Exchange Committee Chair
- Past Member Board of Directors Newark, NY Public Library