U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

December 20, 2021

BY ECF

The Honorable Jesse M. Furman
United States District Judge
Southern District of New York
40 Foley Square
New York, New York 10007

Re: *United States v. Michael Avenatti*, 19 Cr. 374 (JMF)

Dear Judge Furman:

The Government respectfully moves *in limine* to preclude the proffered expert testimony of Donald Vilfer, noticed by defendant Michael Avenatti.[1] For the reasons set forth below, and based on the clear factual record, the proposed testimony of this expert is unreliable and irrelevant, and in any case would serve only to unfairly prejudice the Government, confuse the issues, mislead the jury, and waste time. The proposed testimony should therefore be precluded without a hearing under Federal Rule of Evidence 702. *Atl. Specialty Ins. v. AE Outfitters Retail Co.*, 970 F. Supp. 2d 278, 285 (S.D.N.Y. 2013) ("an evidentiary hearing is unnecessary when the evidentiary record pertinent to the expert opinions is already well-developed").

I. Background

As the Court is aware, the Government has alleged, and expects to prove at trial, that the defendant defrauded his client—Victim-1—by stealing a significant portion of Victim-1's advance on a book contract. The defendant instructed Victim-1's book agent, without authorization and with the use of a fraudulent letter, to send payments not to Victim-1 but instead to a bank account controlled by the defendant. In furtherance of this scheme, the defendant misled Victim-1 about the status of these book payments, including in WhatsApp messages. During its investigation, the Government took screenshots of certain of these messages and Victim-1 provided to the Government an export of the WhatsApp conversation between the defendant and Victim-1. The Government also obtained, pursuant to a court-authorized warrant, the contents of the defendant's iCloud account, which includes thousands of records of WhatsApp calls and text messages between the defendant and Victim-1.

On May 1, 2021, the defendant moved to preclude the Government from offering at trial the screenshots and export of the WhatsApp communications between the defendant and Victim-1.

[1] The defendant's expert notice is attached as Exhibit A.

(Dkt. No. 115.) On September 9, 2021, this Court denied that motion, without prejudice to the defendant lodging "particularized objections to specific exhibits that the Government seeks to introduce at trial." *United States v. Avenatti*, --- F. Supp. 3d ----, No. 19 Cr. 374 (JMF), 2021 WL 4120539, at *3-4 (S.D.N.Y. Sept. 9, 2021). In particular, the Court observed that "it is well established that, if properly authenticated (for example, by a witness with knowledge, such as a participant), screenshots of text messages and copies of electronic communications are admissible." *Id.* at *4.

II. Defendant's Proposed Expert

In an effort to undermine the obvious force of the text messages sent by the defendant to his victim, the defendant proposes the testimony of Vilfer to improperly suggest to the jury, with no basis in fact, nor relevance to any issue at trial, that the Government should have taken some different investigative step with respect to these particular materials and that there is something suspect about them. Specifically, the defendant intends Vilfer to testify that (1) the "best" way to acquire and preserve data is to use Cellebrite or a similar forensic tool to extract data, and (2) PDF files are not "self-authenticating and/or acceptable as evidence of digital data under prevailing professional standards." (Ex. A at 1-2.)

III. Legal Standard

Expert testimony is admissible pursuant to Federal Rule of Evidence 702 if it is "both relevant and reliable." *Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F. Supp. 2d 457, 458 (S.D.N.Y. 2007) (quotation marks omitted). The Court is the "gatekeeper" of such evidence. *See United States v. Rosario*, No. 09 Cr. 415 (VEC), 2014 WL 6076364, at *1 (S.D.N.Y. Nov. 14, 2014). In that role, the Court "must make several determinations before allowing expert testimony: (1) whether the witness is qualified to be an expert; (2) whether the opinion is based upon reliable data and methodology; and (3) whether the expert's testimony on a particular issue will assist the trier of fact." *Tiffany*, 576 F. Supp. 2d at 458 (citing *Nimely v. City of New York*, 414 F.3d 381, 396-97 (2d Cir. 2005)).

Furthermore, even if all these requirements are met, the Court may nonetheless exclude the expert testimony under Federal Rule of Evidence 403 if its prejudicial effect substantially outweighs its relevance. *United States v. Mulder*, 273 F.3d 91, 101 (2d Cir. 2001). "Indeed, the Supreme Court, echoed by members of our own court, has noted the uniquely important role that Rule 403 has to play in a district court's scrutiny of expert testimony, given the unique weight such evidence may have in a jury's deliberations." *Nimely*, 414 F.3d at 397.

Expert testimony is relevant when it "will help the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702(a). Although "Rule 702 embodies a liberal standard of admissibility for expert opinions," *Nimely*, 414 F.3d at 395-96, such testimony "should be limited to situations in which the subject matter is beyond the ken of the average juror," *United States v. Lombardozzi*, No. 02 Cr. 273 (PKL), 2003 WL 1907965, at *2 (S.D.N.Y. Apr. 17, 2003). Accordingly, expert testimony is not proper with respect to "matters which a jury is capable of understanding and deciding without the expert's help." *Andrews v. Metro-North Commuter R.R. Co.*, 882 F.2d 705, 708 (2d Cir. 1989).

The reliability inquiry is flexible and "must be tied to the facts of a particular case." *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 150 (1999). The Second Circuit has emphasized that "it is critical that an expert's analysis be reliable at every step." *Amorgianos v. Nat'l R.R. Passenger Corp.*, 303 F.3d 256, 267 (2d Cir. 2002). "In deciding whether a step in an expert's analysis is unreliable, the district court should undertake a rigorous examination of the facts on which the expert relies, the method by which the expert draws an opinion from those facts, and how the expert applies the facts and methods to the case at hand." *Id.*; *see also id.* at 265 ("[T]he district court should consider the indicia of reliability identified in Rule 702, namely, (1) that the testimony is grounded on sufficient facts or data; (2) that the testimony 'is the product of reliable principles and methods'; and (3) that 'the witness has applied the principles and methods reliably to the facts of the case.'" (quoting Fed. R. Evid. 702)). Minor flaws with an otherwise reliable expert opinion will not bar admission of that evidence; however, the Court should exclude the expert evidence "if the flaw is large enough that the expert lacks 'good grounds' for his or her conclusions." *Id.* at 267 (quotation marks omitted).

At the motion *in limine* stage, the Court should make a preliminary determination under Federal Rule of Evidence 104(a) as to the admissibility of the defendants' proffered expert testimony. *United States v. Nektalov*, No. 03 Cr. 828 (PKL), 2004 WL 1469487, at *1 (S.D.N.Y. June 30, 2004). The proponent has "'the burden of establishing that the pertinent admissibility requirements are met by a preponderance of the evidence.'" *Id.* (quoting Fed. R. Evid. 702 advisory comm. note). The Court may, in its broad discretion, order a factual hearing pursuant to Rule 104 to determine whether expert testimony is reliable under *Daubert v. Merrell Dow Pharma.*, 509 U.S. 579 (1993). However, "[t]he law requires only that the parties have an opportunity to be heard before the district court makes its decision, and an evidentiary hearing is unnecessary when the evidentiary record pertinent to the expert opinions is already well-developed." *Atl. Specialty Ins.*, 970 F. Supp. 2d at 285 (internal citations and quotation marks omitted).

IV. Discussion

The defendant seeks to introduce at trial "expert" testimony that (1) the "best" way to acquire and preserve data is to use Cellebrite or a similar forensic tool to extract data, and (2) PDF files are not "self-authenticating and/or acceptable as evidence of digital data under prevailing professional standards." (Ex. A at 1-2.) Even assuming, *arguendo*, that the Government does offer at trial the screenshots and export of WhatsApp conversations obtained from Victim-1's phone (and not the same material extracted from the defendant's own iCloud account), this testimony would still be unreliable and irrelevant. Moreover, to the extent such testimony did have any plausible relevance to a fact in issue, its probative value would be far outweighed by risk of unfair prejudice, confusing the issues, misleading the jury, and wasting time.

With respect to the proposed testimony regarding the "best" way to deal with electronic data, the testimony will not assist the trier of fact in determining any fact or otherwise understanding any relevant issue at trial. *See* Fed. R. Evid. 702(a). The jury will not be called upon to evaluate or offer its opinion on the Government's selection of investigative tools, and whether data from a phone may be extracted using Cellebrite or the like has no relevance to any fact at issue. *See United States v. Saldarriaga*, 204 F.3d 50, 53 (2d Cir. 2000) ("The jury correctly was instructed that the government has no duty to employ in the course of a single investigation

all of the many weapons at its disposal, and that the failure to utilize some particular technique or techniques does not tend to show that a defendant is not guilty of the crime with which he has been charged.").

Nor would this opinion testimony be reliable. The defendant's expert, who of course had no involvement in the Government's investigation, is prepared to testify regarding the "best" way to gather particular evidence based on his general claim that the software program Cellebrite is most commonly used to acquire digital evidence. (Ex. A at 1 & Vilfer Decl. ¶ 3.) Vilfer is wholly unqualified to offer an opinion as to the "best" manner of gathering evidence in this case, nor is it reliable or useful to a juror to opine that there exists a program that might be used to extract digital data from a seized device and that therefore in the course of any investigation it is "best" to use such a program in all circumstances.

Even if this testimony were relevant or reliable, however, it would be properly excluded under Rule 403. In particular, this testimony would confuse the issues, mislead the jury, and above all, waste time. Were the defendant permitted to call an expert to testify that the Government should have used a particular technique, the Government would be forced to provide testimony and other exhibits to explain to the jury, among other things, how investigations proceed, the use and practice of subpoenas and voluntary requests, when and how the Government executes search warrants for digital evidence, and the Government's customs and practices regarding the obtaining of evidence from witnesses and victims, and would similarly have to elicit testimony regarding the many investigative techniques used in this case, including, for example, obtaining a forensic copy of the defendant's iCloud through a search warrant. In short, this testimony would turn the trial into precisely what it is not and should not be—a review of the Government's chosen investigative techniques rather than an evaluation of whether the defendant's conduct satisfies the elements of the crimes charged.

Similarly, the defendant's proposed testimony that PDF files are not "self-authenticating and/or acceptable as evidence of digital data under prevailing professional standards" (Ex. A at 2) would constitute a wholly improper effort to invade the province of the Court. This Court has already held, consistent with well-established law, that "if properly authenticated (for example, by a witness with knowledge, such as a participant), screenshots of text messages and copies of electronic communications are admissible." *Avenatti*, 2021 WL 4120539, at *4. The defendant nonetheless wishes to call an expert to tell the jury that such materials, even if admitted by the Court, are nonetheless inauthentic. (Ex. A at 2; *see also id.* at Vilfer Decl. ¶ 6 ("I regularly instruct attorneys in the Continuing Legal Instruction classes I teach that paper evidence of electronic files is insufficient and generally not accepted by courts.").)

Moreover, the defendant's intention appears to be to mislead the jury by hinting that there might be something missing or not genuine about the WhatsApp materials by speaking generally about PDF files, while knowing that many—if not all—of the same messages can be located on the defendant's own iCloud account. Indeed, it appears that Vilfer is prepared to testify that it is possible to create "fake" PDF or text files, but not that there is any actual evidence of that being done here. The closest Vilfer comes to such a claim is the bizarre, unsupported, and unreliable assertion that "[m]y review of the printout from Victim-1's attorney also revealed it is clearly incomplete and does not include all of the content of conversations between Mr. Avenatti and

[Victim-1]." The risk of unfair prejudice and confusion is palpable, and the testimony should be precluded under Rule 403 as well.

V. Conclusion

For the foregoing reasons, the Government the Court should preclude the proffered expert testimony of Vilfer based on the record. *Atl. Specialty Ins.*, 970 F. Supp. 2d at 285.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

By: s/ Matthew D. Podolsky
Matthew D. Podolsky
Robert B. Sobelman
Assistant United States Attorneys
(212) 637-1947/2616

cc: Robert M. Baum, Esq. (by ECF)
Andrew J. Dalack, Esq. (by ECF)
Tamara L. Giwa, Esq. (by ECF)

EXHIBIT A

Federal Defenders
OF NEW YORK, INC.

Southern District
52 Duane Street-10th Floor, New York, NY 10007
Tel: (212) 417-8700 Fax: (212) 571-0392

David E. Patton
Executive Director
and Attorney-in-Chief

Southern District of New York
Jennifer L. Brown
Attorney-in-Charge

December 13, 2021

By Email
Matthew Podolsky, Esq.
Robert Sobelman, Esq.
United States Attorney's Office
Southern District of New York
1 St. Andrew's Plaza
New York, NY 10007

Re: United States v. Michael Avenatti
19 Cr. 374 (JMF)

Dear Counsel,

We hereby provide notice pursuant to Federal Rule of Criminal Procedure 16(b)(1)(C) regarding expert testimony that the defense anticipates offering at trial. We reserve the right to supplement this notice with additional expert witnesses and/or additional information concerning the witness disclosed herein.

Donald Vilfer

The defense intends to call Donald Vilfer, an expert on computer and digital forensics. Mr. Vilfer co-owns Vilfer & Associates, Inc., dba Digital Evidence Ventures, a computer forensics and litigation support company headquartered in Roseville, CA. Mr. Vilfer is also a former Supervisory Special Agent with the FBI, last in charge of the white-collar and computer crimes units, including the computer forensics team. Mr. Vilfer has over 30 years' experience as an investigator and expert in the forensic collection, review, and retention of electronically stored information. He also regularly testifies as an expert in state and federal court.

Consistent with the affidavit appended to this notice, and if called to testify, Mr. Vilfer would discuss the tools available to federal law enforcement to obtain forensic copies of electronically stored information, including emails, text messages, and other content from cellular devices. In particular, Mr. Vilfer would testify that in an investigation involving digital evidence, the best way to acquire and preserve data in a manner identical to its original format is to use Cellebrite (or another industry-accepted and proven digital forensic tool) to extract the data. Mr. Vilfer

would also testify about his review of Stephanie Clifford's purported WhatsApp messages with Michael Avenatti, which she gave to the Government, and opine on whether the PDF files are self-authenticating and/or acceptable as evidence of digital data under prevailing professional standards.

In addition to Mr. Vilfer's affidavit, we have attached his curriculum vitae. We currently do not possess any of Mr. Vilfer's prior testimony but will promptly produce any transcripts we obtain.

Sincerely,

/s/
Robert M. Baum, Esq.
Andrew J. Dalack, Esq.
Tamara L. Giwa, Esq.

Counsel for Michael Avenatti

DECLARATION OF DONALD VILFER

I, Donald Vilfer, declare as follows:

1. I am one of the owners at Vilfer & Associates, Inc., dba Digital Evidence Ventures, a computer forensics and litigation support company headquartered in Roseville, California. I am a non-practicing attorney and former Supervisory Special Agent with the Federal Bureau of Investigations, last in charge of the White-Collar Crime and Computer Crimes unit, including the Computer Forensics team. I have over 30 years of experience as an investigator and expert and have provided expert testimony in over 100 cases before Federal and state courts, administrative bodies and the International Trade Commission. I regularly provide Continuing Legal Education training to attorneys in the area of digital forensics and am a Lecturer for the Digital Forensics class at the University of California Davis Master's in forensic science program. Attached is a true and correct copy of my CV. I have personal knowledge of the facts stated in this Declaration and, if called as a witness, could and would testify competently to those facts.

2. In March of 2021, I was retained by the Federal Defenders of New York, Inc. to provide digital forensics services and expert consultation, including evaluating evidence provided in discovery related to WhatsApp messages purportedly sent by defendant along with text messages with other people. I was provided with six pdf files that represented information obtained from the cell phone of Stephanie Clifford. Much of the pdf content consisted of what I was told were photos taken by a government agent of the screen on the phone of Stephanie Clifford. One pdf was a series of photos of a phone screen displaying what appears to be conversations with phone number [redacted] who was listed as "Luke." Another pdf was also a series of photos taken of a phone, showing messages being purportedly sent to number [redacted]. There were no replies from this number in the photos provided. The next pdf was a photo of a phone showing the "About" information for that device, a Galaxy S8 with number [redacted]. Another pdf shows a series of photos of a phone screen with text conversation with number [redacted] referenced as "Elizabeth (Publisher)." The next pdf is a series of photos of a phone, first showing a photo of Michael Avenatti followed by text conversation with a contact of the same name. The final pdf received was an email from Clark Brewster to Matthew Podolsky and Robert Sobelman of the United States Attorney's Office referencing a pdf attachment he calls "the accumulation of text communications between M. Avenatti and Stephanie Clifford covering the time period of his legal representation."

3. Typically in an investigation involving digital evidence, the digital data is acquired using industry-accepted and proven digital forensic tools that preserve the data in an identical format that can later be verified as being the same as the original data stored on the device. In the case of mobile devices, Cellebrite is the most commonly used tool used to acquire the evidence in a forensically sound manner that will allow for later authentication. Cellebrite and similar tools allow for the examiner to not only acquire the files, such as the databases text messages are stored in, but also to recover and document the metadata about the files such as the date created and modified. The tool will also calculate the hash value, often called a digital fingerprint, of the evidence so it can be verified as being the same as what was on the original device, allowing for authentication. In that the tools are forensic tools, they are comprehensive, often recovering deleted messages and all other available communications and information about activity on the device.

4. The pdf files provided by the government fall far short of being acceptable as evidence of digital data. The pdf files depict photos taken of the screen of a phone and offer none of the authenticating information found through the use of forensic tools. With the simple photos of the screen, there is no way to know if the messages are actually associated with the participants or numbers shown. It is very easy to fabricate a series of messages and then change contact information so it appears the messages were with a different person in the contact database. Even if the messages were not fabricated, the selection of what is displayed for a photo of the screen could have been carefully chosen to exclude parts of a conversation or entire conversations. Even prior to the creation of the photos, the user could have deleted select messages to change the context of messages remaining. A forensic extraction of the device could possibly reveal if either of these events occurred.

5. As an example of how unreliable the provided photos are, the photos that begin at Bates USAO374 00007097 first show some highlights of conversations purportedly with the contact Elizabeth. Those highlights include an October 11 message that begins with "It should go up next time too". However, that message is not captured in the provided photos even though the photos include other messages from October 11.

6. The attachment provided by the attorney for Stephanie Clifford is equally problematic. I regularly instruct attorneys in the Continuing Legal Instruction classes I teach that paper evidence of electronic files is insufficient and generally not accepted by courts. The attachment submitted to the government by Stephanie Clifford's attorney consists of a simple string

of text that is titled "WhatsApp chat with Michael Avenetti." WhatsApp is a messaging app used across various digital platforms that stores the messages in a database on the device. Even if a consumer application could be used by someone such as Clifford or her attorney to download messages from the app, the result here appears to be a simple text file that is easily edited. There is no preservation of the conversation that can be authenticated as genuine. Additionally, it is unlikely such an application would recover deleted messages that might be recovered by forensic tools. Whatever was used here to create the text file obviously did not recover conversations with third parties wherein Stephanie Clifford may have discussed the circumstances related to defendant.

7. My review of the printout from Stephanie Clifford's attorney also revealed it is clearly incomplete and does not include all of the content of conversations between Mr. Avenati and Clifford.

8. In investigations that involve digital evidence from mobile devices, the standard practice is to use industry-accepted forensic tools to create a preservation of the data for review. Having received the text file from Clifford's attorney, the best practice would have been for the government agents to then request Clifford's phone for a full extraction. This would have ensured the ability to authenticate the messages, possibly resulted in the recovery of deleted messages and revealed all relevant data that may have been on the device, including discussions with third parties about the allegations or circumstances. The forensic preservation would not have been limited to an export from one app but would have preserved SMS message, MMS or multimedia messages and messages using other apps. This is not what happened in this case. Instead, the government has relied on a text file of questionable origin and photos of Clifford's screen on her phone that those photos by themselves illustrate not all of the messages were collected. The government was in possession of her phone at some point for the photos and could have conducted a forensic preservation to ensure authenticity and completeness but for whatever reason chose not to.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct, and that this declaration was executed on May 1, 2021 in Roseville, California.

Donald Vilfer

Donald E. Vilfer, JD, CFE

Professional:

Vilfer & Associates, Inc., dba Digital Evidence Ventures 2002-present. Founding partner for a Firm that emphasizes computer forensics, eDiscovery and fact-finding in support of complex litigation or referral for prosecution. Representative clients include law firms, state and local government, high-tech firms, aircraft manufacturers, financial institutions and school districts. Cases have included investigation of fraud, theft of intellectual property, computer crimes, employee misconduct, sexual harassment, cell phone location and defense of complex fraud. Extensive experience in obtaining and analyzing computer and cell phone forensic evidence. Experience as an expert witness and court-approved expert in multiple state and Federal jurisdictions as well as the International Trade Commission, having provided sworn testimony over 100 times.

University of California, Davis April 2018-present (full quarter class periodically as scheduled). Lecturer in Digital Forensics for the Masters in Forensics Science Program.

Califorensics 2002-2017. Founder and President of Digital Forensics and Investigative Services firm that served clients nationwide. Sold in 2013 and remained on as Director of Digital Forensics and eDiscovery.

Perry-Smith LLP, 2001-2002, Senior Director, Litigation Support and Investigative Services Group. Led the Litigation Support and Investigative Services practice area for Sacramento's largest regional accounting firm. Supported attorneys in civil and criminal litigation.

Federal Bureau of Investigation, 1986-2001.

1996-2001, Supervisory Special Agent for the White-Collar Crime and Computer Crimes Squad. Conducted and oversaw the investigation of white collar crime and computer crimes. Achieved successful prosecutions in the areas of Securities Fraud, Bank Fraud, Embezzlement, Intellectual Property Rights, Computer Crimes and Bankruptcy Fraud. Oversaw the largest Intellectual Property Rights case in the FBI. Supervised the FBI Computer Forensics Team (CART) and the FBI participation on the High-Tech Task Force. Supervised an international investigation of a series of computer intrusions into financial institutions, resulting in the arrest and conviction of those involved.

1994-1996, Supervisory Special Agent for the Rapid Start Team. At FBI Headquarters, Washington D.C., managed a team of professionals responsible for the on-site management of major cases and crisis worldwide on over 50 cases at venues from the White House to the Oklahoma City bombing command post. Led a project to develop an automated litigation support package for complex white-collar cases. Assisted with implementing automated analysis for Innocent Images project.

1986-1994, Special Agent. Investigated violent crimes, fugitive matters and white-collar crime. Five year FBI SWAT team member. While assigned as Special Agent, Washington D.C. field office, was the case agent an investigation of an international multi-billion dollar bank fraud (BCCI). Oversaw a team of agents and financial analysts responsible for gathering relevant evidence and tracing proceeds. Conducted investigation and asset tracking throughout the US, England, the Cayman Islands and Abu Dhabi.

Donald E. Vilfer, JD, CFE
(continued)

As Assistant Division Counsel, provided legal advice and instruction to FBI Agents in criminal, civil, and employment law areas. Reviewed affidavits for search warrants and court orders.

Delaware Ohio County Prosecuting Attorney's Office, 1986. Prosecuted criminal cases and successfully briefed and argued an appeal.

Education: Bachelor of Science, Criminal Justice/Pre-Law, Bowling Green State University, 1982.

Ohio State University College of Law, Juris Doctorate, 1986.
National Moot Court Team member, advancing to the national level.

Specialized Training: Access Certified Examiner (ACE) certification for Computer Forensics and Decryption.

Certified in Physical and Logical Analysis of cell phones and mobile devices along with additional training in cell phone location evidence.

Four months training at the FBI Academy, including courses in White Collar Crime.

50 Hour Certified Fraud Examination course, including investigation, computer crime, law and accounting. Received CFE Certification.

Advanced White-Collar Crime courses during tenure with the FBI.

One week Computer Crimes course for FBI Supervisors.

Advanced Computer Forensics training, including Windows Registry analysis and Mac OS forensics. Incident Response (hacking) training.

Network Forensics and Cell Phone Location training.

FBI Computer Security class.

FBI class for Supervisory Special Agents over Computer Crimes investigations.

Continuing Legal Education Instructor, *Computer Forensics for Attorneys* and other courses

Frequent guest and consultant to media on crime and computer forensics matters.

FBI Instructor for International Law Enforcement Training Academy in Budapest.

Publication: Incorporating Cell Phone Data into Your Investigations
The AWI Journal-September Vol. 9 No. 3 (2018)

Affiliations: Member of the Ohio Bar (inactive status).
Member of the Association of Certified Fraud Examiners.

Expert Testimony: Federal Courts, State Courts, FINRA, California Office of Administrative Hearings, International Trade Commission.