Corporate Articles

published by Corporate & Association Counsel Division
of the Federal Bar Association

Winter 2016

An Interview with Carolyn St. Clair: Changes to the Federal Rules of Civil Procedure and the Impact on the Discovery Rules

by Rachel V. Rose, JD, MBA

RR: Please share your litigation background with us.

CS: For the past 28 years, I have practiced civil trial law, focusing on mass tort litigation and personal injury. I also served as a briefing attorney for the Texas Supreme Court for one year.

RR: What are your most memorable cases?

CS: There are so many memorable clients, but some of the cases that received global media coverage and resulted in positive changes resulting from the litigation stand out: Jessica Santillan, a teenaged girl who died from receiving mismatched blood donor organs during a heart/lung transplant; Dr. Hitoshi Nikaidoh, a medical doctor decapitated by a miswired hospital elevator; a young girl severely burned during the Brennan's Restaurant fire; the children of the engineer who fell to his death working on the Houston Rockets scoreboard; the medical device and toxic exposure cases I am working on now (IVC blood clot filters, transvaginal mesh, hip implants and the Deepwater Horizon Oil spill) have already resulted in product and industry changes. I can go on and on.

RR: In April, Chief Justice Roberts sent the Reports of the Committee on Rules of Practice and Procedure to the Judicial Conference of the United States containing the Committee Notes submitted to the Court for its consideration pursuant to Section 331 of Title 28, United States Code to Congress. How will the changes to FRCP 26 impact both plaintiffs and defense counsel, especially in class action litigation?

CS: The changes are designed to force

In This Issue

Message from the Chair

by Rachel V. Rose, JD, MBA

To paraphrase Brad Paisley, every year, you get 365 blank pages to write a book. Write a good one!

It is with this sentiment in mind that I and the other members of the Corporate and Association Counsel Division's Leadership Team approach 2016. Reflecting on 2015, we found steady growth in our membership, received positive feedback from you, our membership, on the content of our newsletter and discovered a multitude of topics to address in 2016. Thank you for your ideas and participation in the CACD.

Regardless of whether you litigate or assist outside counsel with various proceedings, every attorney needs to be aware of the recent changes to the Federal Rules of Civil Procedure. We, the CACD, have addressed this on two fronts. First, Caroyln St. Clair, an experienced litigator has contributed an article to this edition of the newsletter. Second, I had the opportunity to interview Arthur Miller, the renowned civil procedure expert on certain facets of the changes. That interview appears in *The Federal Lawyer.*

We were also fortunate to have Lauren Lucht Abney interview Robert Wittman, the author of Priceless, founder of the FBI's art crime division and our upcoming, featured CLE speaker. Having heard him present, I can attest that his presentation is amazing and will lead to great discussions with clients and colleagues alike.

Finally, every professional and company needs to be aware of cybersecurity issues. One "hot topic" that has graced a multitude of publications is phishing. I hope that you read Chris Cochran's article with particular interest, given his experience with military and corporate cybersecurity issues. There are some excellent tips to incorporate into training and to help mitigate risk.

In sum, we plan on "writ[ing] a good one" and we hope that you do, too! ■

plaintiffs and defense counsel to communicate, cooperate and create a case management discovery plan early in the litigation. The discovery plan must be submitted to the court within 14 days after the attorneys confer. In class actions, a damage analysis upfront may assist in calculating whether the proposed cost of discovery exceeds the potential range of recovery. The concept set forth is that a case management session at the beginning of litigation, considering the proportionality factors, will prevent excessive expense and waste of judicial resources involving vexatious discovery disputes.

RR: Please define "proportionality" in the context of FRCP 26 and its impact on discovery.

CS: "Proportionality" replaces the former term, "reasonably calculated" in response to complaints that the latter term allowed the discovery process to spiral out of control. FRCP 26 states that discovery can be obtained relevant to any party's claim or defense and proportional to the needs of the case. The proportionality factors to be considered include: the importance of the issues at stake in the action; the parties' relative access to relevant information; the parties' resources; the importance of the discovery in resolving the issues; and whether the burden or expense of the proposed discovery outweighs its likely benefit. The information need not be admissible to be discoverable and the burden is not on the requesting party to defend the proportionality of its request.

RR: What impact will these changes have on e-discovery?

CS: Electronically stored information (ESI) will be addressed at the discovery plan conference with an agreement regarding any issues about disclosure, discovery, or preservation of ESI, including the form in which it should be produced. If the ESI is deemed not reasonably accessible due to undue burden or expense, the burden is on the party resisting production to prove it is inaccessible. For good cause shown, the requesting party will be able to obtain the inaccessible ESI, but may be responsible for some or all of the cost. The requesting party should have an IT specialist consulted about the true costs and ability of accessing the ESI, to counter the producing party's objection. In the event that a party has accidentally produced privileged material, the requester must promptly return, sequester, or destroy the specified information and any copies, then take reasonable steps to retrieve any information already distributed. Any party found negligently destroying evidence can be sanctioned by preclusion of their evidence and introduction of the parties failure to preserve the evidence that was destroyed. More severe sanctions can be imposed when it is proven a party has intentionally destroyed evidence.

RR: What professional and/or personal accomplishments are you most proud of?

CS: Maintaining a successful solo law practice since the 80's and receiving the Distinguished Alumnus Award from the University of Texas Health Science Center of Nursing. ■

Dangers of Phishing

by Chris Cochran

Imagine for a moment that you are the head of security for an office building. You have sole authority over the selection and implementation of security solutions to protect the building from unauthorized entry. You choose fences as an external barrier, badge readers at all external doors, security guards at every turnstile, cameras, motion sensors and other bells and whistles to protect the building. It has become your own personal Fort Knox. Then, one day, one of your security guards sees a man running in the door. The man says to the guard, "I need to get in now! There has been a breach and your boss has summoned me to contain it!" The security guard did not waste a moment. He let the man in, hoping that he would be able to protect his new employer. Unbeknownst to the security guard, the man was actually hired to infiltrate the building. The man was not lying. There had been a breach. And it was just allowed by the security guard.

What happened in this story? The head of security (you) built a strong security architecture, only to be undermined by misdirection and a lack of awareness. This is what happens when an end user opens a phishing email and clicks one of the links or opens a malicious attachment. This attack bypasses all of those well thought out, top-of-the-line security solutions that you or your information security personnel implements to protect the network and its residing information. This provides the adversary with the desired access to the network.

There are several types of phishing. The focus of this article involves the primary types: phishing, spear phishing and whaling. Phishing is simply the sending of masqueraded email in the hopes of getting the recipient to behave in the interest of the attacker. This behavior could range from providing full credentials to clicking links or opening malicious documents to affect computers or networks for follow-on attacks. Phishing attacks can be disseminated widely as spam to hundreds or thousands of email addresses and are constructed to appeal to a wider audience. On the other hand, spear phishing is more targeted and requires more tailoring, hence "spearing." Whaling is even more targeted, usually pursuing the compromise of executive level accounts or systems. These operations also have a variety of desired outcomes.

There is a full-spectrum of motivations for phishing operations. The primary motivation for phishing is to enable the theft of money or information. The e-crime underground is full of sellers and buyers of stolen credit card numbers, compromised computer system shells (computers that have been previously compromised by another hacker) and other confidential information for the uses of fraud and other illegal activities. Medical information

is a prime target due to the amount of sensitive information in medical records. Sensitive information is not only sought after for it's intrinsic value, but also its impact on society or organizations. Hacktivists execute attacks to build a narrative for their ideology, usually to embarrass or simply reveal sensitive data. This makes legal documents a prime target as they contain relationships, conditions of cooperation and acquisition details. As one can see, phishing can be devastating to individuals and organizations, but there are mitigations against this threat.

The biggest defense against these attacks is awareness. Individuals need to be aware of the types, motivations and mitigations of phishing campaigns and operations. Adversaries use domains that look like legitimate domains used everyday. Individuals should check the spelling of websites (ie myhat[.]com vs myhaat[.]com]) and hover (please do not click) their mice over hyperlinks to reveal true destinations. If an individual is not expecting an email and the email is requesting sensitive data or requesting the opening of an attachment or the clicking of a link it may be worth it to call the sender and verify its legitimacy. There are also technical mitigations such as not conducting daily work as an administrator (which is a powerful account that enables the installation of programs and other system changes) and application whitelisting (this allows only predetermined applications to be executed on a system).

As information security improves and it becomes harder to intrude on a network, the bad guys are finding ways for individuals to provide them with the access. The adversary has a lot to gain from an individual's or an organization's information. Awareness and other mitigations makes those devastating attacks harder to execute and may save money, time and peace of mind. ■

Mr. Cochran is a former US Marine with over a decade of Signals Intelligence/ All-Source Intelligence Analysis experience and a deep passion for security. He began conducting Cyber Threat Intelligence analysis in 2010 and founded Ashlar Cyber Solutions in 2015. Mr. Cochran has led Cyber Threat Intelligence analysis teams at the tactical, operational and strategic level. He has provided threat intelligence council to the highest levels of government and Industry and built Threat Intelligence capabilities for organizations across multiple sectors.

Document Retention and Destruction Requirements in Relation to HIPAA and ERISA

by Ryan C. Temme, JD and Rachel V. Rose, JD, MBA

Introduction

Whether it is the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[1] the Employee Retirement Income Security Act of 1974 ("ERISA")[2] or the Sarbanes-Oxley Act of 2002 ("SOX"),[3] all of these laws and the related rules have data retention, policy and procedure and data destruction requirements. The increase in data breaches, both paper and electronic, as well as administrative actions being taken by the U.S. Securities and Exchange Commission (SEC), the U.S. Department of Health and Human Services Office for Civil Rights (HHS-OCR) and precedent setting case law,[4] underscore the importance of having adequate policies and procedures that establish the relevant timeframes for retention, as well as the proper protocols for destroying the sensitive information.

This article provides an overview of the requirements in relation to HIPAA and ERISA, while recognizing that different sectors (e.g., healthcare) and public companies may have unique situations to consider. Practical take-aways on data destruction requirements and policy and procedure contents are also provided. In sum, the goal is to provide counsel and compliance officers with a comprehensive starting point for evaluating this important aspect of business.

Requirements of HIPAA and ERISA

HIPAA protects the security and confidentiality of health data by imposing obligations on covered entities, such as health plans (including self-insured group health plans), and health care providers. Entities covered by HIPAA's requirements must ensure that health information protected by HIPAA, known as protected health information ("PHI"), remains secure and, if health information is breached, follow certain breach protocols set forth under HIPAA. HIPAA's Privacy rule generally applies to all PHI,[5] while the Security Rule applies specifically to electronic PHI (or "ePHI").[6]

In reality, access to health information is not always limited to the covered entity itself. To assist with business functions, health plans and employers contract with other entities such as third-party administrators (who process claims and make available networks of providers) ("TPAs"), law firms, consultants, and actuarial firms. Depending on the nature of services they provide, these other entities may have access to PHI.

To ensure that PHI is protected, HIPAA requires that health plans enter into business associate agreements with service providers that may have access to PHI. Business associate agreements generally provide that the business associate will comply with the requirements of HIPAA and require the business associate to impose the same compliance obligations on any sub-contractor that the business associate may engage to help with plan-related activities.

Importantly, HIPAA itself does not prescribe the method for retaining or destroying PHI. As a result covered entities retain have some leeway in designing policies and procedures that are designed to comply with HIPAA Privacy and Security Rule. A thorough review of health plan related activities should be undertaken to ensure that group health plan, employer, and business associate practices meet the requirements of both the Privacy Rule and the Security Rule.

Under ERISA, the plan sponsor of an employee benefit plan

faces a series of reporting and disclosure requirements. Notably, the annual report, or Form 5500, requires that plans submit significant detail on a number of facets of the plan and its administration. Section 107 of ERISA in turn requires that plans maintain sufficient records to verify, explain, clarify, and check for accuracy and completeness of the disclosed information for a period of not less than six years after the filing date of the disclosure documents.[7] In the event that the records are lost, stolen or destroyed, the Department of Labor requires the plan to reconstruct the records to the extent that doing so would be possible at a reasonable cost.[8]

If an employer sponsors a pension plan, then ERISA also requires that employer to "maintain records with respect to each of his employees sufficient to determine the benefits due or which may become due to such employees" and to supply those records to the plan administrator upon request.[9]

Data Destruction and Policy Take-Aways

A good place to begin is with an adequate risk assessment. After a recent HHS HIPAA violation, Jocelyn Samuels, director of HHS' Office for Civil Rights indicated, "[a]ll too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical record or that fails to provide appropriate oversight and accountability for all parts of the enterprise."[10] Whether electronic medical records, employee records containing sensitive personally identifiable information, or paper records, a comprehensive risk assessment is crucial. Next, the requisite timeframes, as identified herein, need to be expressly included in the policies and procedures. When a timeframe is unidentified, a safe timeframe to retain a document is seven years in relation to HIPAA, employee medical benefits and employee medical histories, as well as other related records and correspondence. [11] And, when state law provides a longer period of retention than federal law, use the longer time period.

From there, specific contents of policies need to be constructed. Two crucial areas that need to be included in document retention and destruction policies are the documents within a specific department and the requisite retention period. For example:[12]

ACCOUNTING SYSTEMS	Retemtion Period
Accounts Payable Ledger	7
Charts of Accounts	Perpetuity
HUMAN RESOURCES	Retention Period
Employee Medical History	7
Employee Medical Benefits	7

Now that the timeframes for retention have been identified, what are the appropriate ways to destroy the documents? According to the National Institute of Standards and Technology ("NIST"), "[m]edia sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort."[1] The ultimate goal is to maintain the confidentiality of the information after its "useful life" has expired. Given that the loss of confidentiality equates to the unauthorized disclosure of the information, which in turn triggers breach reporting protocols in a variety of laws, making sure that the sensitive information (e.g., PHI and PII) is destroyed in an appropriate manner is crucial.[2] NIST publication 800-88r1 details the requirements that are referenced in a variety of laws. In turn, these standards should be incorporated into policies and procedures. Overall, it is crucial to understand the relevant timeframes of each law for data retention, compile comprehensive policies and procedures and adhere to the requisite standards when destroying information to maintain its confidentiality.

Conclusion

A comprehensive risk assessment can be the first step in determining whether or not the requisite data retention and destruction standards have been addressed. The next step is to create a chart of the document requirements of the industry that the company is in and to meet the requirements for publically traded companies. Finally, making sure that the policies and procedures are comprehensive and updated at least annually can help to mitigate liability. In sum, this is one area that cannot be left unaddressed. ■

Ryan C. Temme, JD, is the vice-chair of Chapter Relations and an associate at The Groom Law Group. He can be reached at rtemme@groom.com.

Rachel V. Rose, JD, MBA is the chair of the FBA's Corporate and Associations Counsel Division and the co-author of What are International HIPAA Considerations? *and* The ABCs of ACOs. *She can be reached at* rvrose@rvrose.com.

Endnotes

[1]Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (Aug. 21, 1996).

[2]Employee Retirement Income Security Act of 1974, Pub. L. 93–406, as amended through Pub. L. 114–74, enacted Nov. 2, 2015.

[3]Sarbanes-Oxley Act of 2002, Pub. L. 107-204 (2002).

[4]*See*, www.beckershospitalreview.com/legal-regulatory-issues/learning-from-wall-street-how-healthcare-providers-can-benefit-from-jpmorgans-london-trading-experience.html; and www.physicianspractice.com/articles/end-year-hipaa-fines-underscore-compliance (last accessed, Dec. 15, 2015).

[5]45 CFR § 164.500, *et seq.*

[6]45 CFR § 164.302, *et seq.*

[7]29 U.S.C. § 1027.

[8]DOL Adv. Op. Ltr. 84-19A (Apr. 26, 1984).

[9]29 U.S.C. § 1059(a)(1).

[10]*See,* www.modernhealthcare.com/article/20151214/NEWS/151219937/university-of-washington-medicine-reaches-750000-hipaa-settlement (last accessed, Dec. 15, 2015).

[11]SOX §210.2-06 (including memos, correspondence and emails).

[12]*See* www.cpa.net/resources/retengde.pdf (outlining different departments, individual types of documents and retention periods).

[13]National Institute of Standards and Technology, *Special Publication 800-88r1*, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf (last accessed, Dec. 18, 2015).

[14]*Ibid.*, *citing*, "Definitions," Title 44 *U.S.Code*, Sec. 3542. 2006 ed. Supp. 5, *available at*, www.gpo.gov/.

Priceless—An Interview with Robert Wittman, Founder of the FBI's Art Crime Division

by Lauren Lucht Abney

1) Tell me about your background. How did you end up having a passion to recover stolen art for the U.S.?

I started as an FBI agent in 1988. The reason I wanted to join the FBI was because Miami Vice was on television at the time, and I liked the show. I thought the FBI would be the group that would do that type of detective work on boats near the water. However, I ended up in Philadelphia, far from boats and water. I was put on the crime squad involving high-jackings between New York and Miami. There was a lot of crime that went on between the two cities. The first art theft cases I was assigned to were in Philadelphia. Two of my first cases were an armed robbery from the Rodin Museum and one from the University of Pennsylvania.

The piece stolen from the Rodin Museum was taken at gunpoint in 1988. The work of art was Auguste Rodin's sculpture, "Man with the Mask of the Broken Nose." This was a critical work in the history of art because it was the first piece created in the impressionist period, and it initiated the impressionist movement. Rodin created the sculpture in the 1860s by accident. He was working in Paris in a barn that had no heat, creating works of art to submit to the standard academy. The sculpture was patterned after the head of a lowly worker named Bebe. Due to the cold temperatures in the barn where Rodin was working, the head cracked in half and the back half of the head fell off of the sculpture. Rodin decided to submit the cracked head to the academy in its broken form. It was a huge success, and the piece was considered to be avant guard. The "Man with the Mask of the Broken Nose" started Rodin's successful career.

I was assigned the Rodin case along with the University of Pennsylvania case. The University case was a crystal ball owned by the Dowager Empress Cixi of China. The University of Pennsylvania had acquired the crystal ball in the 1930s. It was the second largest crystal ball in the world. It was stolen in a burglary, and was worth $350,000 at the time. I solved both of these cases, and so I started getting all the art theft cases assigned to me. At that time there was no art crime team. The FBI was investigating art theft cases just like regular theft cases, such as a car theft.

Art crime is not about art history, it is about the business of art. Today, the art business is a $200 billion industry for legitimate art sales, and $6 billion in illegitimate dealings. The United States is the largest art market in world, and comprises 40% or $80 billion a year of the world's art market. To put it in perspective, all professional sports revenue combined is only $26 billion a year.

2) Did being raised by an antiques dealer influence your passion for art history?

Yes. I knew how to make an art deal because my parents owned three antique stores when I was growing up. They specialized in selling Asian antiques. My mother was a Japanese citizen working on an air force base during the Korean War, and my father met her on base over there. Growing up in an antiquities environment was important because it taught me how to do an art deal under cover when I got to the FBI. I knew the lingo, and knew more about making art deals than the criminals did. The criminals did not specialize in art theft cases. They were common criminals committing all types of theft, such as assault, car theft, and bank robberies. They just happened to be doing an art theft at the time. They didn't necessarily know how to do art deals.

3) Tell me about the development of the FBI's art crime division? How did you end up as senior investigator?

Between the years 1988 and 2005, I worked on art theft cases all over the world in 20 different countries. I worked a case in Sweden, and came back to States and realized there was no specialized training here to learn how to recover stolen art. Art theft investigations are very different from car thefts and other types of theft. So I went to FBI headquarters and asked if they would create a team for art crime. They said yes, and put me in charge of it because I had been solving art crime cases for my entire career. I put together a team, and created a specialized program to train agents to investigate art theft. The unit started with 8 agents, and had a small budget. The training was formalized, and the first one took place in Philadelphia. We took the agents to museums to teach them about antiquities. We took them to the Barnes Foundation to give them an appreciation of techniques that would aid in the identification of different artists' styles, and we took them to the Philadelphia Museum of Art for conservation training. The FBI still has this training every year. The agents travel to different cities to study investigation techniques and to study art. Today, the FBI's art crime team has 14 collateral duty agents, and has recovered $150 million worth of stolen art since I started the team in 2005.

4) What has been your most exciting and rewarding case?

I can't really give you an answer to that because all of the art I recovered is valuable and important. The most valuable piece I helped recover was a Bill of Rights owned by the state of North

Corporate Articles is published by the Corporate & Association Counsel Division of the Federal Bar Association, 1220 North Fillmore Street, Suite 444, Arlington, VA 22201. Managing Editor: Yanissa Pérez de León.

Carolina. It was signed by George Washington. The document was stolen by a union trooper in 1865. This was the oldest theft I was involved in. The value of the piece at the time we recovered it in 2003 was $100 million. Of course, it can't be sold because it is owned by the state of North Carolina.

Another memorable case was the recovery of a U.S. Civil War battle flag. It was carried into battle by one of the first African American regiments in the Battle of Fort Hudson during the Civil War. Both of these pieces are such an important part of our history.

5) What was your role in reclaiming Nazi stolen art?

The FBI didn't do much of that. Those are civil cases, and the FBI specializes in criminal cases. Nazi stolen art cases are based on ownership, and not really considered thefts because the people who now have them did not steal them, and were involved in good faith transactions to buy or inherit them. The title procedures on how to make a claim to recover Nazi stolen art are covered in war treaties and international law rather than U.S. laws.

6) Where does corporate law and art law intersect? Can you describe the affect corporate law has had on any of your cases?

Corporations have large art collections sometimes for tax purposes, education of clients, or the owners enjoy the art. Tax laws are all in play with corporations. Art collections are the property of the corporation and protected by the corporation; they are not owned by individuals. Dealers and auction houses are all corporations too. It's the same for selling and buying art whether it is an individual or a corporation. Corporations can either be victims of art theft or be investigated for theft themselves. I had a case where an insurance company suffered an art theft from a corporation's headquarters. The former CEO of the company stole many pieces of art from the corporation's collection. It happens all the time. I've had three cases that dealt with insurance fraud. Museum curators steal art too.

7) What laws or regulations, in your opinion, should either be promulgated or repealed in order to preserve America's art history and ease the recovery of stolen art?

I think the laws are fine. There are plenty of laws that deal with art theft. The issue is whether or not people pay attention to them, and whether they use the laws to prosecute the criminals. It is a question of commitment by law enforcement to uphold the statutes and investigate the thefts. They are viewed many times as victimless crimes, but that is not true. There are victims when art is stolen. Sometimes the victims are insurance companies, and when they pay for the lost art we all suffer because our premiums increase. We are all victims of it financially, and we are also victims because it is a cultural loss for all of humanity when a piece is stolen from a museum. It's a piece of genius we no longer have access to.

8) What is your latest book about?

It is titled, The Devil's Diary, and is about recovering the private diary of Alfred Rosenberg who was the chief civil scientist for Hitler during WWII. Alfred Rosenberg was in charge of taking art from the Jews in Europe. He stored it and compiled it to put in the Fuhrer Museum. He also took all of their private belongings with him back to Germany. He came up with the idea of Holocaust, and was with Hitler from 1919 to 1945 until Hitler died.

A 500 page diary he had written was discovered during the Nuremberg trials. He was hung and the diary went missing. It was taken by a prosecutor at the trial. There are only three diaries that exist that were written by high-ranking Nazi officials.

We found the diary in upstate New York. The secretary of the prosecutor had the diary in her possession. I started the case in 2001 and we recovered it in 2013. The diary had never been translated before we recovered it. The diary is now in the U.S. Holocaust Museum in Washington D.C. The Devil's Diary comes out on March 29th, 2016, and is published by Harper Collins.

9) What are you currently working on besides your book?

I still recover artwork. I provide different art services to clients such as collection management, art theft recovery, security and recovery, and I create reports for clients regarding due diligence to see if their art practices have been executed correctly. I make sure clients procure art legally, make sure it's authentic and that they have the proper contracts to create works of art.

10) Any concluding remarks?

The theft of a Rembrandt self-portrait from the Swedish National Museum in Stockholm is a good reminder of how important it is to recover stolen art. I worked with the Swedish police and the Danish government to recover a Rembrandt self-portrait and two Renoirs that were stolen at gunpoint during the daytime in 2000. We recovered all three of them in Copenhagen. One Renoir was recovered in 2001, and the other Renoir and Rembrandt self-portrait were recovered in 2005. At the time of recovery all three paintings were in the hands of different criminals. This case illustrates the importance of cultural property, and the need for governments to work together in order to recover these priceless pieces for the benefit of society. ■

Federal Bar Association Application for Membership

The Federal Bar Association offers an unmatched array of opportunities and services to enhance your connections to the judiciary, the legal profession, and your peers within the legal community. Our mission is to strengthen the federal legal system and administration of justice by serving the interests and the needs of the federal practitioner, both public and private, the federal judiciary, and the public they serve.

Advocacy
The opportunity to make a change and improve the federal legal system through grassroots work in over 90 FBA chapters and a strong national advocacy.

Networking
Connect with a network of federal practitioners extending across all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands.

Leadership
Governance positions within the association help shape the FBA's future and make an impact on the growth of the federal legal community.

Learning
Explore best practices and new ideas at the many Continuing Legal Education programs offered throughout the year—at both the national and chapter levels.

Expand your connections, advance your career

THREE WAYS TO APPLY TODAY: Join online at www.fedbar.org; Fax application to (571) 481-9090; or Mail application to FBA, PO Box 79395, Baltimore, MD 21279-0395. For more information, contact the FBA membership department at (571) 481-9100 or membership@fedbar.org.

Applicant Information

First Name M.I. Last Name Suffix (e.g. Jr.) Title (e.g. Attorney At Law, Partner, Assistant U.S. Attorney)

❍ Male ❍ Female Have you been an FBA member in the past? ❍ yes ❍ no Which do you prefer as your primary address? ❍ business ❍ home

Business

Firm/Company/Agency Number of Attorneys

Address Suite/Floor

City State Zip Country

( )

Phone Email Address

Home

Address Apt. #

City State Zip Country

( ) / /

Phone Date of Birth

Email Address

Bar Admission and Law School Information (required)

U.S.
Court of Record: _____
State/District: _____ Original Admission: / /

Foreign
Court/Tribunal of Record: _____
Country: _____ Original Admission: / /

Tribal
Court of Record: _____
State: _____ Original Admission: / /

Students
Law School: _____
State/District: _____ Expected Graduation: / /

Authorization Statement

By signing this application, I hereby apply for membership in the Federal Bar Association and agree to conform to its Constitution and Bylaws and to the rules and regulations prescribed by its Board of Directors. I declare that the information contained herein is true and complete. I understand that any false statements made on this application will lead to rejection of my application or the immediate termination of my membership. I also understand that by providing my fax number and e-mail address, I hereby consent to receive faxes and e-mail messages sent by or on behalf of the Federal Bar Association, the Foundation of the Federal Bar Association, and the Federal Bar Building Corporation.

Signature of Applicant ***Date***

(Signature must be included for membership to be activated)

*Contributions and dues to the FBA may be deductible by members under provisions of the IRS Code, such as an ordinary and necessary business expense, except 4.5 percent which is used for congressional lobbying and is not deductible. Your FBA dues include $15 for a yearly subscription to the FBA's professional magazine.

Federal Bar Association

Application continued on the back

Membership Categories and Optional Section, Division, and Chapter Affiliations

Membership Levels

Sustaining Membership

Members of the association distinguish themselves when becoming sustaining members of the FBA. Sixty dollars of the sustaining dues are used to support educational programs and publications of the FBA. Sustaining members receive a 5 percent discount on the registration fees for all national meetings and national CLE events.

	Private Sector	Public Sector
Member Admitted to Practice 0-5 Years	❍ $165	❍ $145
Member Admitted to Practice 6-10 Years	❍ $230	❍ $205
Member Admitted to Practice 11+ Years	❍ $275	❍ $235
Retired (Fully Retired from the Practice of Law)	❍ $165	❍ $165

Active Membership

Open to any person admitted to the practice of law before a federal court or a court of record in any of the several states, commonwealths, territories, or possessions of the United States or in the District of Columbia.

	Private Sector	Public Sector
Member Admitted to Practice 0-5 Years	❍ $105	❍ $80
Member Admitted to Practice 6-10 Years	❍ $165	❍ $140
Member Admitted to Practice 11+ Years	❍ $210	❍ $170
Retired (Fully Retired from the Practice of Law)	❍ $105	❍ $105

Associate Membership

Foreign Associate

Admitted to practice law outside the U.S. ❍ $210

Law Student Associate

First year student (includes four years of membership) ❍ $50
Second year student (includes three years of membership) ❍ $30
Third year student (includes two years of membership) ❍ $20
One year only option ❍ $20

All first, second and third year student memberships include an additional free year of membership starting from your date of graduation.

Dues Total: _____

Practice Area Sections

- ❍ Admiralty Law $25
- ❍ Alternative Dispute Resolution $15
- ❍ Antitrust and Trade Regulation $15
- ❍ Banking Law $20
- ❍ Bankruptcy Law $25
- ❍ Civil Rights Law $10
- ❍ Criminal Law $10
- ❍ Environment, Energy, and Natural Resources $15
- ❍ Federal Litigation $20
- ❍ Government Contracts $20
- ❍ Health Law $15
- ❍ Immigration Law $10
- ❍ Indian Law $15
- ❍ Intellectual Property Law $10
- ❍ International Law $10
- ❍ Labor and Employment Law $15
- ❍ Qui Tam Section $15
- ❍ Securities Law Section $0
- ❍ Social Security $10
- ❍ State and Local Government Relations $15
- ❍ Taxation $15
- ❍ Transportation and Transportation Security Law $20
- ❍ Veterans and Military Law $20

Career Divisions

- ❍ Corporate & Association Counsel (in-house counsel and/or corporate law practice) $20
- ❍ Federal Career Service (past/present employee of federal government) N/C
- ❍ Judiciary (past/present member or staff of a judiciary) N/C
- ❍ Senior Lawyers* (age 55 or over) $10
- ❍ Younger Lawyers* (age 40 or younger or admitted less than 10 years) N/C
- ❍ Law Student Division N/C

*_**For eligibility, date of birth must be provided.**_

Sections and Divisions Total: _____

Chapter Affiliation

Your FBA membership entitles you to a chapter membership. Local chapter dues are indicated next to the chapter name (if applicable). If no chapter is selected, you will be assigned a chapter based on geographic location. *No chapter currently located in this state or location.

Alabama
- ❍ Birmingham
- ❍ Montgomery
- ❍ North Alabama

Alaska
- ❍ Alaska

Arizona
- ❍ Phoenix
- ❍ William D. Browning/ Tucson–$10

Arkansas
- ❍ Arkansas

California
- ❍ Inland Empire
- ❍ Los Angeles
- ❍ Northern District of California
- ❍ Orange County
- ❍ Sacramento
- ❍ San Diego
- ❍ San Joaquin Valley

Colorado
- ❍ Colorado

Connecticut
- ❍ District of Connecticut

Delaware
- ❍ Delaware

District of Columbia
- ❍ Capitol Hill
- ❍ D.C.
- ❍ Pentagon

Florida
- ❍ Broward County
- ❍ Jacksonville
- ❍ North Central Florida–$25
- ❍ Orlando
- ❍ Palm Beach County
- ❍ South Florida
- ❍ Southwest Florida
- ❍ Tallahassee
- ❍ Tampa Bay

Georgia
- ❍ Atlanta–$10
- ❍ Southern District of Georgia Chapter

Hawaii
- ❍ Hawaii

Idaho
- ❍ Idaho

Illinois
- ❍ Central District of Illinois
- ❍ Chicago
- ❍ P. Michael Mahoney (Rockford, Illinois) Chapter

Indiana
- ❍ Indianapolis
- ❍ Northern District of Indiana

Iowa
- ❍ Iowa–$10

Kansas
- ❍ Kansas and Western District of Missouri

Kentucky
- ❍ Kentucky

Louisiana
- ❍ Baton Rouge
- ❍ Lafayette/ Acadiana
- ❍ New Orleans–$10
- ❍ North Louisiana

Maine
- ❍ Maine

Maryland
- ❍ Maryland

Massachusetts
- ❍ Massachusetts –$10

Michigan
- ❍ Eastern District of Michigan
- ❍ Western District of Michigan

Minnesota
- ❍ Minnesota

Mississippi
- ❍ Mississippi

Missouri
- ❍ St. Louis
- ❍ Kansas and Western District of Missouri

Montana
- ❍ Montana

Nebraska*
- ❍ At Large

Nevada
- ❍ Nevada

New Hampshire
- ❍ New Hampshire–$10

New Jersey
- ❍ New Jersey

New Mexico
- ❍ New Mexico

New York
- ❍ Eastern District of New York
- ❍ Southern District of New York
- ❍ Western District of New York

North Carolina
- ❍ Eastern District of North Carolina
- ❍ Middle District of North Carolina
- ❍ Western District of North Carolina

North Dakota
- ❍ North Dakota

Ohio
- ❍ Cincinnati/ Northern Kentucky-John W. Peck
- ❍ Columbus
- ❍ Dayton
- ❍ Northern District of Ohio–$10

Oklahoma
- ❍ Oklahoma City
- ❍ Northern/ Eastern Oklahoma

Oregon
- ❍ Oregon

Pennsylvania
- ❍ Eastern District of Pennsylvania
- ❍ Middle District of Pennsylvania
- ❍ Western District of Pennsylvania

Puerto Rico
- ❍ Hon. Raymond L. Acosta/ Puerto Rico–$10

Rhode Island
- ❍ Rhode Island

South Carolina
- ❍ South Carolina

South Dakota
- ❍ South Dakota

Tennessee
- ❍ Chattanooga
- ❍ Knoxville Chapter
- ❍ Memphis Mid-South
- ❍ Nashville
- ❍ Northeast Tennessee

Texas
- ❍ Austin
- ❍ Dallas–$10
- ❍ El Paso
- ❍ Fort Worth
- ❍ San Antonio
- ❍ Southern District of Texas–$25
- ❍ Waco

Utah
- ❍ Utah

Vermont*
- ❍ At Large

Virgin Islands
- ❍ Virgin Islands

Virginia
- ❍ Northern Virginia
- ❍ Richmond
- ❍ Roanoke
- ❍ Hampton Roads Chapter

Washington*
- ❍ At Large

West Virginia
- ❍ Northern District of West Virginia–$20

Wisconsin*
- ❍ At Large

Wyoming
- ❍ Wyoming

Chapter Total: _____

Payment Information

TOTAL DUES TO BE CHARGED
(membership, section/division, and chapter dues): $ _____

❍ Check enclosed, payable to Federal Bar Association
Credit: ❍ American Express ❍ MasterCard ❍ Visa

Name on card (please print)

Card No. Exp. Date

Signature Date