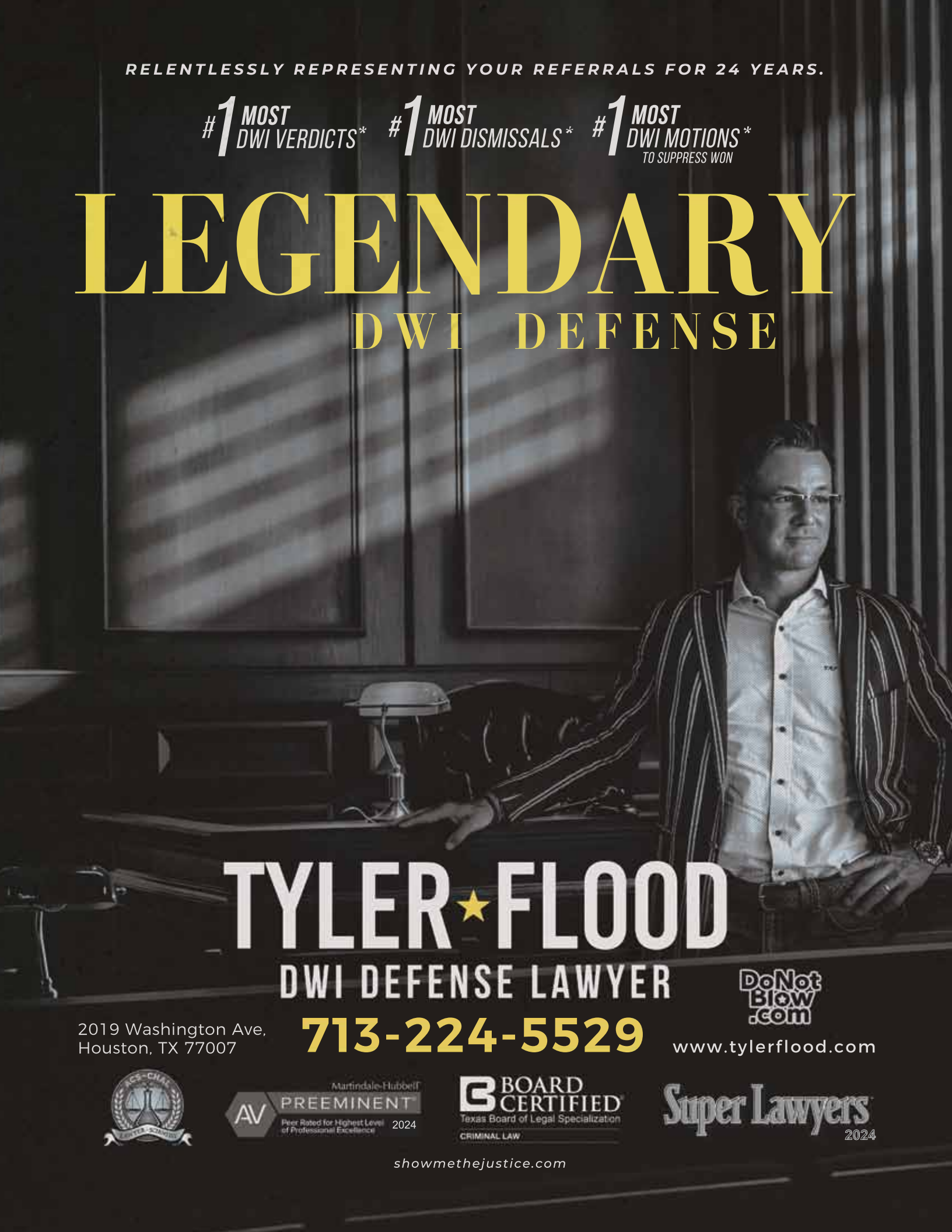
THE HOUSTON lawyer
Volume 62 – Number 5
March/April 2025

# Cybersecurity Law


RELENTLESSLY REPRESENTING YOUR REFERRALS FOR 24 YEARS.
#1 MOST DWI VERDICTS*
#1 MOST DWI DISMISSALS*
#1 MOST DWI MOTIONS* TO SUPPRESS WON
LEGENDARY
DWI DEFENSE
TYLER FLOOD
DWI DEFENSE LAWYER
DoNotBlow.com
2019 Washington Ave,
Houston, TX 77007
713-224-5529
www.tylerflood.com
ACS-CHAL
Martindale-Hubbell
AV PREEMINENT
Peer Rated for Highest Level of Professional Excellence 2024
BOARD CERTIFIED
Texas Board of Legal Specialization
CRIMINAL LAW
Super Lawyers 2024
showmethejustice.com

# BEST LAW FIRMS IN AMERICA

**TODD FRANKFORT**
**PARTNER**

**BEST LAW FIRMS**
RANKED BY Best Lawyers

OWLAWYERS®
TRIAL LAW
*The Wise Choice®*
OWLAWYERS.COM

- DALLAS
- FORT WORTH
- FRISCO
- HOUSTON

HOUSTON:
19 BRIAR HOLLOW LN., STE. 200
HOUSTON, TX 77027
T: (713)-224-1800

PRINCIPAL OFFICE: 1845 WOODALL RODGERS FRWY, STE 1525, DALLAS, TX 75201
BEST LAW FIRMS IS A REGISTERED TRADEMARK OF WOODWARD/WHITE, INC.

# CONTENTS

**March/April** 2025 **Volume 62 Number 5**







## FEATURES



*The Houston Lawyer* (ISSN 0439-660X, U.S.P.S 008-175) is published bimonthly by The Houston Bar Association, 1000 Louisiana St., Suite 3600, Houston, TX 77002. Periodical postage paid at Houston, Texas. Subscription rate: $12 for members. $25.00 non-members. POSTMASTER: **Send address changes to: *The Houston Lawyer*, 1000 Louisiana St., Suite 3600, Houston, TX 77002. Telephone: 713-759-1133.** All editorial inquiries should be addressed to *The Houston Lawyer* at the above address. **All advertising inquiries should be addressed to: Quantum/SUR, 10306 Olympia Dr., Houston, TX 77042, 281-955-2449 ext 1,** www.thehoustonlawyer.com, e-mail: leo@quantumsur.com.

# CONTENTS

**March/April** 2025 **Volume 62 Number 5**





## DEPARTMENTS

**By DAVID HARRELL**
**Troutman Pepper Locke LLP**

# Harris County's Pressing Need for New District Courts

Earlier this year, Harris County Commissioners voted in favor of asking Texas lawmakers to create five more civil district courts. The Houston Bar Association supports and applauds this decision. Ensuring we have a more adequate number of district courts serving our residents underscores core pillars of the HBA's mission—providing access to justice and promoting the rule of law. While the request to the Texas Legislature falls short of the nine courts originally proposed to Harris County Commissioners Court in February, it's still a step forward to address a dire need in our justice system.

> ***"Yet, while Harris County is home to 4.8 million people, it only has 24 district courts, 11 family courts, and three juvenile courts. As a result, litigants wait longer for resolution, even as judges are asked to work harder."***

Texas' pro-business drive over recent years has seen an estimated 16.4% population boom over the last 15 years. During that time, 25,000 businesses relocated to Texas. Those businesses, and the residents they employ and serve, have increased the demand on Harris County District courts. Yet, while Harris County is home to 4.8 million people, it only has 24 district courts, 11 family courts, and three juvenile courts. As a result, litigants wait longer for resolution, even as judges are asked to work harder. It is difficult to deliver on a pro-business message and attract investment in the Houston area when the courts are prevented from providing essential judicial services.

A letter the HBA submitted to Harris County Commissioners in February noted the inadequate number of district courts:

- The 38 district courts spanning the civil, family, and juvenile divisions is well short of the estimated 69 courts needed across those three divisions, based upon a 2023 study by the National Center for State Courts (NCSC).
- Harris County has operated with 24 Civil District Courts for almost four decades, so filings per court have dramatically increased with no increase in the number of courts.
- In 2024, Harris County has almost 3,100 new cases filed per court, more than any district court system in Texas.
- Despite Harris County district courts closing almost 3,000 cases per court, the number of pending cases increased in 2024.

Adding five civil district courts would be the first increase in civil district courts in over 40 years. While 29 civil district courts falls well short of the estimated 50 needed for Harris County, it will reduce the number of cases per court to 2,400 (still 20% higher than the number of new filings per civil district court in Dallas County) and allow courts to reduce the backlog of pending cases.

But Harris County needs more. Harris County needs 16 family courts; it has 11. It has only 29 of the needed criminal district courts. Meanwhile, an additional juvenile court is necessary because filings have increased by 30% since 2020.

The creation of new district courts is long overdue. Testimony before Commissioners Court in favor of creation of new courts reminded us that "justice delayed is justice denied," a statement often quoted when we argue why an efficient legal system is so crucial. Creating new district courts would support investment in Harris County and aid the delivery of essential judicial services to Harris County residents and businesses. More is needed, but Harris County Commissioners have taken a laudable step in the right direction.

**By ANDREW PEARCE**
**BoyarMiller**

# CYBERSECURITY: Putting IT Into the Practice of Law



I am truly excited to introduce you to this month's issue, but I first want to address an omission from our last issue, in which we spoke with lawyers who have practiced for 25 years to ask what they know now that they wish they had known when their legal careers first started. Unfortunately, we failed to include **Justice Brett Busby**'s quote. Justice Busby, a current Justice of the Supreme Court of Texas and a former Justice of the 14th Court of Appeals, shared the following:

*The most effective advocates (1) get to the point and help busy judges find the best answer, and (2) avoid distracting and ineffective tactics like attributing bad motive to the other side—e.g., accusing them of "misleading" the court. Show why you're right, don't tell that they're bad.*

When I realized I had failed to include his submission, I immediately reached out to offer my sincere apologies and to let Justice Busby know we would highlight his quote in our next issue. As comes as no surprise to those who know him, Justice Busby could not have been more kind or gracious. I am glad I have this opportunity in my column to relay his thoughts to our readers.

Turning to this issue, we wanted to focus on cybersecurity. I remember when I graduated from college in 1995 and the internet was in its infancy. I think I had a university email account, but I am quite certain I never used it. Similarly, I was aware of the internet, but I do not recall anything of significance in those early days. Almost a decade later, I was about to enter law school and the world had changed. Email had become an essential means of communicating, and the internet was becoming the platform for everything from banking to shopping to search engines to the start of social media.

It was almost impossible to conceive of the amount of change that had occurred in such a short span of time. Fast forward another 20 years or so and the change in technology has only continued to explode in ways that very few could imagine.

Against this backdrop, we are proud to bring a series of articles from an outstanding group of authors on the rise of cyber threats and the best practices for both lawyers and their clients to deal with them, if not avoid them altogether. **Lynn Sessions**, **Kimi Gordy**, **Jessica Lowery**, and **Pierce Cox** discuss their experiences over the past year in privacy and cybersecurity, explore some landmarks in the current environment, and make a few predictions on possible future developments. **Alamdar Hamdani** and **Lucy Porter** introduce us to a variety of tools used by cybercriminalsto steal information and generally cause havoc. **Innovative Driven**, an alternative legal support provider, focuses on cybersecurity in the legal industry, highlighting the rising number of breaches and spotlighting the need for all-sized firms to adopt strong cybersecurity measures to protect client confidentiality and maintain trust.

**Laura L. Ferguson**, in turn, brings us up to speed on the Texas Data Privacy and Security Act, which recently went into effect in Texas.

We also have some great contributions to our regular features, including a wonderful profile of **David Barron**'s hiking adventures around the world by **Carey Worrell**. Readers can also learn about the HBA's Fee Dispute Committee by **Felicia Harris Hoss**, the HBA's Law Practice Management Section by **Shannon Almes**, a legal update on *DeVillier v. Texas* from **Cassie McGarvey**, and an informative piece on the Harris County Responsive Interventions for Change Docket by **Eric Benavides**, who does a great job of introducing us to the RIC Court.

Finally, I want to highlight **Rinku Ray**'s review of *The Man Behind the Robe: A Personal Reflection and Review of Scalia: Rise to Greatness, 1936–1986* by Jeffrey Rosen. Rinku did a terrific job of framing the review based upon the dissonance she saw between the man and the robe which, as she says, "sparked a deeper curiosity" in her and led her to ask: Who was Justice Scalia, really? As any fan of Ted Lasso will recall, and as Rinku wonderfully reminds us, we should all strive to "be curious, not judgmental."

As always, I want to express my sincere appreciation to everyone who contributed to this issue, including the associate editors and board members who made it happen, as well as a special thank you to **Braden Riley**, who did a terrific job serving as this issue's guest editor.

By ALAMDAR HAMDANI and LUCY PORTER

## IN THE CROSSHAIRS OF CYBERCRIMINALS –

# Houston's Infrastructure Industries Are Under Attack


On December 25, 2009, I[1] moved from Kentucky to Washington, D.C. to join the Department of Justice's Counterterrorism Section and its Al Qaeda Unit, joining an international effort to bring Al Qaeda's terrorists to justice. At the time, U.S. intelligence agencies considered Al Qaeda the country's primary national security threat.[2] In fact, on that Christmas morning more than 15 years ago, while I drove into Washington for the first time, a Nigerian national, Umar Farouk Abdulmutallab, arrived in Detroit attempting to ignite a bomb hidden in his underwear on behalf of Al Qaeda in the Arabian Peninsula—an Al Qaeda affiliate based in Yemen.[3] Although passengers subdued Abdulmutallab before he could cause any harm, he brought home the notion that Al Qaeda was still a threat to the homeland more than eight years after the September 11, 2001 attacks.

Much has changed since then. According to the U.S. intelligence community, the People's Republic of China ("China") has eclipsed Al Qaeda as the largest national security threat, and instead of attacking us with bombs, planes, or martyrs, China, Russia, North Korea, and criminal organizations—often working with nation-states—deploy weapons that don't target physical structures, but rather the nation's cyber network.[4] And they are primarily targeting America's businesses with a focus on America's critical infrastructure.

According to the Cybersecurity and Infrastructure Security Agency ("CISA"), a U.S. federal agency responsible for safeguarding national cybersecurity and protecting critical infrastructure against threats, "[t]here are 16 critical infrastructure sectors . . . so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[5] Cybersecurity in these industries is crucial since any disruption or breach can lead to significant impacts on public safety, the economy, and national security. Four critical infrastructure sectors call Houston home—energy, health care, transportation (including the Port of Houston and two major airports), and a large concentration of chemical manufacturing companies. It is why Houston's businesses and public utilities are on the front lines of America's war against cyberattacks from government actors and criminal organizations.

Cybercriminals use a variety of tools—phishing, malware, ransomware (a type of malware), and insider threats—to steal information and to generally cause havoc. Ransomware is a particularly powerful tool, allowing a cybercriminal to encrypt a victim's files, then demand a ransom for the decryption key. Ransomware can paralyze systems, disrupt operations, and inflict financial loss. Ransomware has become so effective that it is now an underground industry, offered as a service called Ransomware as a Service (RaaS).[6] Through this business model, ransomware developers offer their ransomware code to affiliates (for a fee), which allows the affiliates to launch their own ransomware attacks. The RaaS business model enables developers to increase their profits beyond running attacks themselves.

A stark example of a ransomware attack on a key infrastructure industry occurred early in 2024, when a hacking group with ties to Russia known as BlackCat or ALPHAV instituted a hack that crippled a portion of the health care system and exposed the data of 190 million Americans—or

more than half the U.S. population.[7]

Change Healthcare, owned by UnitedHealth Group, manages health care technology pipelines and "acts as a clearing house for 15 billion medical claims each year—accounting for nearly 40 percent of all claims."[8] In February 2024, BlackCat used stolen credentials to gain initial access to Change Healthcare's network. These credentials provided access to a server that did not have multifactor authentication enabled; a security process that requires users to verify their identity through multiple methods—such as a password, a fingerprint, or a verification code—before gaining access to a system or account. Once inside, the attackers moved within the network, exploring and gaining access to various systems and data. BlackCat then exfiltrated a vast amount of sensitive data undetected before deploying the ransomware.[9] The ransomware encrypted files and disabled large portions of Change Healthcare's operations, causing widespread chaos for weeks, which included critical functions such as claims processing, prescription management, payment, prior authorization, and insurance verification. Hospitals reported delays in authorizations and disbursements causing financial strains. According to a survey by the American Hospital Association, "[n]early all hospitals (94%) said they have suffered a financial impact from the Change Healthcare attack [and] [n]early 60% of the hospitals said the impact on their revenue has been $1 million per day or greater."[10] Eventually, Change Healthcare paid a $22 million ransom to obtain a decryption key and prevent the publication of stolen data. Despite the payment, the cybercriminals retained the stolen data, and the attack had lasting implications for the health care industry.[11]

### Attacks on Third-Party Vendors

Besides attacks directly to a company's systems, vendors are also a vector of attack. For example, in December 2020, hackers associated with the Russian government infiltrated the systems of SolarWinds, an IT management company, and planted malware giving them backdoor access to the networks of SolarWinds' clients. Many of SolarWinds' clients were U.S. government agencies, and by compromising SolarWinds, the attackers were able to move laterally into the systems of more than 18,000 organizations, including key federal agencies, such as the Department of Homeland Security, the State Department, and the Departments of Commerce and the Treasury. The attack highlighted the vulnerabilities in software supply chains, chains outside of a company's internal cyber infrastructure; vulnerabilities exploited by both cyber criminal enterprise and hostile nation-state actors.[12]

### Nation-State Sponsored Attacks

Nation-state actors possess advanced tools and capabilities developed or acquired through significant investment in research and development. Like cyber criminal enterprises, they deploy a range of tactics, from phishing and malware to sophisticated exploitation of software vulnerabilities. But unlike the cyber criminal enterprises, their actions are not just aimed at financial gain but are part of a broader strategy to disrupt, destabilize, and gather intelligence. A key feature of state-sponsored groups is the patience to plan for the long-term. The most sophisticated nation-state actor is China.

### China-Sponsored Attacks

China's goal is to assert geopolitical leverage so it can surpass the U.S. as the world's leading global superpower, and by targeting critical infrastructure, China seeks to gather intelligence, exploit vulnerabilities, and potentially disrupt operations in times of conflict or heightened tension. In essence, when the time is right, "wreak havoc and cause real-world harm to American citizens and communities."[13]

That came to light with a group associated with China's military, Volt Typhoon. Discovered in 2023, the Volt Typhoon hackers employed advanced stealth techniques to infiltrate various organizations. They infected old Small Office/Home Office (SOHO) routers, due to weak passwords, outdated firmware, or unpatched software. By controlling SOHO routers, Volt Typhoon established a covert command and control infrastructure that deployed malware

within a targeted network without arousing suspicion, since traffic to and from these devices appeared legitimate.[14] Volt Typhoon then used the SOHO router cover to surreptitiously gain access into critical infrastructure systems ready to likely, as former FBI Director Wray testified, "wreak havoc."[15]

While the Volt Typhoon campaign was in full swing, another China state-sponsored hack, the Salt Typhoon espionage campaign, was also underway. This hacking campaign began as early as 2022 and infiltrated the U.S. telecommunications infrastructure, compromising the systems of at least nine major providers, including AT&T and Verizon. This sophisticated attack, deemed the "worst telecom hack in U.S. history" by Senate Intelligence Committee Chairman Mark Warner, exploited vulnerabilities in outdated network devices, such as Cisco routers, to gain persistent access, harvest metadata, intercept unencrypted communications, and even targeted phones used by high-value government individuals, including President Donald Trump and Vice President J.D. Vance during the recent presidential campaign.[16]

## Impacts of Cyber Incidents

Unfortunately, the Change Healthcare, SolarWinds, and Volt Typhoon hacks are examples of hacks that occur every day on critical infrastructure industries, including Houston's—attacks that have the potential to cost businesses millions. Houston's companies must prepare for the inevitable cyber attack. According to IBM's "Cost of a Data Breach Report 2024", the average cost of a data breach rose in 2024 to $4.88 million from $4.45 million in 2023, due to both direct and indirect costs of responding to a breach.[17] Direct costs include operational downtime and the associated financial losses, as well as the costs to address the cyber incident itself, such as ransomware payments, regulatory fines, call center costs, or consumer protection measures. Indirect costs may include loss of customers, loss of reputation, or increased insurance premiums. For incidents involving critical infrastructure, the incident could result in public and environmental safety risks, such as threats to human life due to disruptions to essential services. These risks make critical infrastructure a continued focus for regulation and a target for threat actors.

## Preparation Strategies

Cybersecurity is not the sole responsibility of your IT group but is an organization-wide effort. A first step in developing a good cybersecurity defense is building into your organization cybersecurity best practices. Best practices may differ depending on the size and nature of your organization, but there are several organizations that provide frameworks for cybersecurity: NIST Cybersecurity Framework,[18] North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection,[19] ISO 27001, and ISO 27032.[20]

Generally, best practices include technical security measures, training, periodic audits and assessments, and recommended policies and procedures to implement, maintain, and improve cybersecurity programs. Technical security measures include access controls, encryption, and software updates that may be solely in the purview of an entity's IT team. Training should include appropriate risk identification training for employees at every level of an organization. Audits and assessments can include both internal and external assessments and may include penetration testing or gap assessments.

## Responding to Cyber Incidents

One procedure that is critical for preparing for a cyber incident is an incident response plan—a guide for responding in the event of a cyber incident. A cyber incident response plan can borrow from other emergency response plans depending on the industry. A key component is identifying the internal team that will assemble in the event of an incident. NIST guidance includes steps for communications with outside parties, including external team members, preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.[21] A great way to prepare for a cyber incident is to perform tabletop exercises, which gather the internal team in simulated events, and can test the effectiveness of different aspects of your plan.

The size and nature of your internal team will depend on your organization, but may include representatives from IT, legal, finance, human resources, public relations, outside counsel, and forensic experts. External communications may include notifications to insurance providers, law enforcement, regulators, and affected individuals (*e.g.*, consumers or customers).

Insurance policies that cover cyber security risks, or cyber insurance, can be a key component of a cyber risk management strategy. But like all aspects of cyber risk management, it is critical that an organization understand the components of a cyber insurance policy. First, you and your broker must identify the types of events that should be covered. Understanding whether your industry is susceptible to ransomware attacks, cyber extortion events, or privacy claims can help tailor a policy to your business. Beyond the policy amounts, it is important to understand the requirements for invoking coverage. Effective cyber claims often require following a specific set of procedures, including making proper notifications and maintaining proper documentation. Advantageously, cyber insurance policies often provide access to experts that can assist in the event of an attack. One such expert is a ransomware negotiator.

As threat actors become more sophisticated, the response to their attacks has become correspondingly specialized. One role that has been crucial for responding to threat actors has been the ransomware negotiator. Much like a hostage negotiator, ransomware negotiators engage directly with the threat actor to negotiate the terms of settlement. Ransomware negotiators possess specialized knowledge of the threat actor landscape, often having detailed knowledge of individual attackers. They possess the technical skills to analyze the impact of an attack and can provide tools to assess the potential damage and aid with recovery. And they provide expertise on "industry" trends enabling you to get context for the scope of your payment.

Law enforcement can also be an important partner in identifying a threat actor. The FBI strongly encourages voluntary reporting to its Internet Crime Complaint Center at ***ic3.gov***. Notification can unlock investigative resources, decryption tools, and coordination with entities like the U.S. Secret Service or Interpol, potentially miti-

gating damage or recovering assets. This can be especially important because paying ransoms—which is not illegal under U.S. law unless funding sanctioned groups—doesn't guarantee data recovery and may invite further attacks. Also, law enforcement can use its many tools to identify the bad actors, bank accounts, bitcoin wallets, and decryption keys. A key ingredient to law enforcement's success is speed, so the sooner a victim notifies law enforcement, the better.

Law enforcement uses many investigative tools to recover monies, identify perpetrators, and launch cyber tools to counteract attacks. These tools include grand jury subpoenas to banks and telecommunication companies, secured communications with foreign law enforcement partners, and sealed search warrants that remove malware. This work is done in secret and under seal. Despite that, companies fear reporting to law enforcement could lead to public exposure or regulatory scrutiny, so companies often weigh reporting against operational secrecy. Best practice leans toward notifying law enforcement for support and to bolster broader cyber defense, but it's a judgment call unless specific breach thresholds or sector rules require notification.

## Regulatory Notification

Timing and extent of notification to regulators depends on applicability of any rule and nature of the data compromised. Every state has a breach notification law requiring notification to consumers in the event personal data is compromised and many of these also require notification to the state attorney general. Many agencies, including the Securities and Exchange Commission, the NERC, the Department of Energy, Department of Defense, Department of Health and Human Services, and the Transportation Safety Administration (maintains pipeline security), and CISA, require notification or disclosures in the event of a cyber incident. Also, many foreign regulators require notifications that may conflict with or contradict the notifications required by the U.S. agencies, making it imperative that multi-nationals understand their global reporting regime. In essence, the regulatory notification scheme is complicated, making it important to have a plan in place post-breach with the assistance of experienced legal counsel.

## Conclusion

On a snowy Christmas Day, just over 15 years ago, I began my career as a national security prosecutor. It started with me chasing Al Qaeda terrorists hiding in camps nestled in the mountains and hills of Afghanistan and Yemen and ended in Houston as the U.S. Attorney, where I led a cadre of prosecutors and investigators dedicated to disrupting hackers hiding behind encryption keys and keyboards in China and Eastern Europe. Over that time, I had to adapt as the threats became more complex, the attacks more constant, and the attackers more sophisticated. Although today's hackers are spread throughout the globe, their focus remains on Houston, targeting the businesses that serve the nation's critical infrastructure needs while caring little for the safety of the citizens that rely upon those key industries.

***Alamdar Hamdani** is a litigation partner at Bracewell, LLP concentrating on government enforcement, white collar criminal defense, cybersecurity, and commercial litigation. Prior to joining Bracewell, Alamdar served in the Department of Justice, most recently as the United States Attorney for the Southern District of Texas.*

***Lucy Porter**, a counsel in Bracewell's Houston office, advises clients on matters related to protecting their technology and information assets. She works with clients to develop and implement bespoke data privacy solutions that are compliant with global regulations, and she has experience working across organizations, including compliance, HR, security, IT, and legal.*

## Endnotes

1. The first-person accounts throughout this article are from Alamdar. I appreciate my co-author allowing me the opportunity to share my story.
2. Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence, 111th Cong. (2010) (statement of Dennis C. Blair), https://isis-online.org/uploads/conferences/documents/2010_NIE.pdf.
3. BBC, *Underwear Bomber Abdulmutallab Sentenced to Life*, Feb. 15, 2012, https://www.bbc.com/news/world-us-canada-17065130.
4. Annual Threat Assessment of the U.S. Intelligence Committee, Office of the Dir. of Nat'l Intelligence, Feb. 5, 2004, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.
5. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *Critical Infrastructure Sectors* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited Mar. 18 2025).
6. CROWDSTRIKE, *Ransomware as a Service (RAAS) Explained How It Works & Examples*, https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (last visited Mar. 18, 2025).
7. HEALTHCARE INNOVATION, *Change Healthcare Tallies 190 Million Data Breach Victims*, Jan. 27, 2025, https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/55263828/change-healthcare-tallies-190-million-data-breach-victims (last visited Mar. 18, 2025).
8. ENERGY & COMMERCE COMM., *What We Learned: Change Healthcare Cyber Attack*, May 3, 2024, https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack (last visited Mar. 18, 2025).
9. *Examining the Change Healthcare Cyberattack: Hearing Before the House Committee on Energy & Commerce*, 118th Cong. (2024) (statement of Andrew Witty).
10. MEDICAL ECONOMICS, *Change Healthcare Breach Affected 100,000,000 Patients*, Oct. 28, 2024, https://www.medicaleconomics.com/view/change-healthcare-breach-affected-100-000-000-patients (last visited Mar. 18, 2025).
11. SECURITY INTELLIGENCE, *Change Healthcare Discloses $22M Ransomware Payment*, May 24, 2024, https://securityintelligence.com/news/change-healthcare-22-million-ransomware-payment/ (last visited Mar. 18, 2025).
12. TECHTARGET, *SolarWinds Hack Explained: Everything You Need to Know*, Nov. 3, 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (last visited Mar. 18, 2025).
13. *Hearing Before the House Select Committee on Strategic Competition between the United States and the Chinese Communist Party*, 118th Cong. (2024) (statement of Christopher Wray).
14. Press Release, U.S. Dept. of Justice, U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure (Jan. 31, 2024), https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.
15. *See, supra*, note 13.
16. Ellen Nakashima, *Top Senator Calls Salt Typhoon 'Worst Telecom Hack in Our Nation's History'*, Wash. Post, Nov. 21, 2024, https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/.
17. IBM, Cost of a Data Breach Report 2024, https://www.ibm.com/reports/data-breach (last visited Mar. 18, 2025).
18. NAT'L INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cybersecurity Framework*, https://www.nist.gov/cyberframework (last visited Mar. 18, 205).
19. NERC, *Standards*, https://www.nerc.com/pa/Stand/Pages/Default.aspx (last visited Mar. 18, 205).
20. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO 27001:2022); INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Cybersecurity—*Guidelines for Internet Security* (ISO 27032:2023).
21. NAT'L INSTITUTE OF STANDARDS AND TECHNOLOGY, *Computer Security Incident Handling Guide*, NIST SP 800-61r2 (2012); NAT'L INSTITUTE OF STANDARDS AND TECHNOLOGY, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, NIST SP 800-61r3 (2024).

By LYNN SESSIONS, KIMI GORDY, JESSICA S. JOHNSON, and PIERCE COX

## A YEAR OF PRIVACY AND CYBERSECURITY:

# A Look Back, A Look Around, and A Look Ahead

As the digital landscape continues to evolve and technology advances, privacy and cybersecurity remain central concerns for individuals, businesses, and regulators. There have been significant developments in privacy regulations and government enforcement actions, major data security incidents, and cybersecurity innovations. From the rise of sophisticated ransomware attacks to the implementation of new state privacy laws, the landscape has been marked by both challenges and progress. Here, we discuss our experience in the past year in privacy and cybersecurity, explore some landmarks in the current environment, and make a few predictions on possible future developments.

### A Look Back at 2024

In April, BakerHostetler will publish its eleventh annual Data Security Incident Response Report ("DSIR Report"), distilling insights and metrics from more than 1,250 data incidents our firm helped clients manage in 2024. The DSIR Report is designed, in part, to help develop cybersecurity measures, incident response plans, and information governance practices. Some highlights from our current analysis of the DSIR Report data are below.

#### Ransomware preparedness and response may be improving.

Ransomware has long been a scourge, and the effects of an attack can be devastating. Unprepared organizations hit with ransomware encryption may need weeks to recover full functionality. During this time, the attack may be highly visible, and the encryption can make it difficult or impossible to deliver for clients, customers, and other stakeholders. Compounding these challenges, threat actors often engage in a double-extortion model: data is exfiltrated prior to encryption and payment demanded not only for a tool to decrypt, but also to prevent publication of the stolen information. Victim organizations also must inform affected individuals and regulators according to applicable data breach notification laws.

In 2024, though, the effects of ransomware attacks were somewhat suppressed. Most of the network intrusions our firm handled in 2024 involved both data theft and ransomware encryption. Even so, the proportion of victims that paid a ransom to purchase a decryption tool did not increase significantly when compared to 2023, and in 2024, the time to recover from a ransomware attack once again saw a year-over-year decrease. This suggests organizations are continuing to improve backup management and recovery processes, as the availability of and time to recover from viable backups can be key drivers for an organization evaluating whether to pay a ransom. Additionally, compared to 2023, the cost and time to complete a forensic investigation both decreased in 2024, and fewer ransomware events involving data theft resulted in notice to individuals. This may show not only that forensic investigators are increasingly efficient, but also that organizations continue to implement information management strategies that help control unauthorized access to sensitive data.

Ransomware continues to be a risk, but organizations appear to be implementing measures that can reduce the impact of an attack. Multifactor authentication ("MFA") and a properly configured endpoint detection and response tool ("EDR") can help prevent access or detect potentially malicious activity. Managing access permissions to the minimum necessary for a user's role and auditing accounts to remove privileges not needed can help to contain threats in the event of a network intrusion. Appropriate data retention poli-

cies and procedures can help to prevent the exposure or exfiltration of sensitive data. Consistently following best practices for backup procedures and testing, such as the "3-2-1 backup rule" (three copies: one live/in production; two others on different devices/media; one of those at an offsite location), can help to eliminate the need for a decryption tool and reduce recovery time in the event of ransomware encryption.

### A renaissance for large fraudulent fund transfers?

Unauthorized actors use a variety of techniques to gain access to systems and networks, but social engineering continues to be a leading cause of financial loss for organizations. As an example of one common method, an attacker may send a phishing email purporting to be from a known or legitimate source with a link to access a document or view a secure message. The link takes the recipient to a webpage that appears legitimate, such as a spoofed Microsoft login page, and asks them to sign in to review the content. Upon entering their credentials, the recipient sees a login error but has granted an unauthorized actor access to their email account.

Phishing attacks such as this were a significant vector for unauthorized actors to gain access to email accounts in 2024. As a potential corollary, 2024 also saw an increase in the total amount of funds diverted by criminals when compared to 2023, as well as the average amount that was the subject of a misdirected transfer. After gaining access to an email account, unauthorized actors were seen to impersonate counterparties to change payment instructions and divert funds. They concealed their activity from users by creating rules to hide legitimate messages from the real counterparty.

Organizations can help to protect against these kinds of attacks by employing technical solutions, adding additional controls, and raising awareness. Multifactor authentication, voice-verification for changes to payment instruction and post-transfer verbal confirmation, and additional employee training and testing of protocols are all measures that can help to reduce the risk of financial loss at the hands of an email phisher.

### Vendor incidents are still a risk that must be managed.

Once again in 2024, approximately 25% of the incidents we saw involved assisting clients with managing the impacts of outside vendors and service providers. This trend shows no sign of slowing. We continue to assist clients whose service providers had high-profile incidents, such as Change Healthcare and Snowflake; attacks on software and systems, such as secure file transfer protocol applications ("SFTPs"), including Accellion, MOVEit, and Cleo (among others); and other third parties, such as managed service providers. The continuing prevalence of third-party data incidents highlights the importance of incorporating a robust vendor management program into information management and cybersecurity strategies.

To manage risks posed by third-party service providers, organizations should consider three key elements for their vendor management program: pre-selection diligence, contractual standards, and performance oversight. Assessing and classifying the risk level of each vendor through questionnaires, onsite reviews, audits, or third-party risk scoring should be a regular part of pre-engagement diligence. After a vendor is selected for engagement, the contract terms should address the organization's privacy and security needs, which may include provisions concerning the data elements involved, the availability of the data to the organization, the vendor's business continuity plan, and the rights and obligations of each party in the event of a data incident at the vendor. During the engagement, the organization should undertake to monitor and review the vendor's performance to ensure that the agreed-upon measures and practices are in place and, when the engagement ends, take the appropriate steps to ensure its data is secure to mitigate or eliminate the impacts in the event the vendor has a post-engagement incident.

## Current Trends in Privacy and Cybersecurity

### *Comprehensive Privacy Legislation: The New Black-Letter Law Sweeping the Nation*

While certain federal laws govern privacy

in particular industries or in connection with some types of transactions, the United States Congress has yet to pass generally applicable federal privacy legislation. State legislatures are filling the gap with their own comprehensive privacy laws that address consumer privacy rights and business obligations.

California passed the first such law in 2018, the California Consumer Privacy Act ("CCPA"), and 19 states now have a comprehensive consumer privacy law on the books. Seven of these were signed into law in 2024. The Texas Data Privacy and Security Act ("Texas DPSA"), which is the Texas comprehensive consumer privacy law, was passed in 2023 and became effective in July 2024. Comprehensive privacy laws become effective in seven more states in 2025. There are also 14 states with comprehensive privacy laws at some stage of the legislative process.

While the scope of comprehensive privacy laws varies by state, laws typically recognize that consumers have the right to access, correct, or delete personal information maintained by a business (or "data controller"), to opt out of having their personal information processed, and to request their personal information be disclosed to them in a common file format for portability. Many also require the data controller to provide notice to consumers about how their data will be used, make opt-in (rather than opt-out) the default position for sale of personal information of consumers under a certain age, conduct formal risk assessments of their privacy and security measures, and prohibit discrimination against consumers exercising their rights under these laws.

Some states have comprehensive privacy laws featuring unique provisions. For example, Oregon's comprehensive privacy law allows an individual to request a list of third parties to which the data controller discloses their personal data. The Texas DPSA states that it applies to any business which produces goods or provides services to a resident of Texas that is not a "small business" under the U.S. Small Business Administration standards, rather than establish applicability based on a certain threshold of data processed.

In short, a federal comprehensive privacy law may lay beyond the horizon. For now, state legislatures are taking up the mantle to put forward and pass legislation for their own constituencies. The result has been a patchwork of regulations, some of which include novel approaches, which can present compliance challenges.

### *New Frontiers in State Investigation and Enforcement*

As comprehensive privacy laws become more widespread across the nation, state attorneys general are ramping up their enforcement efforts. Texas has been notably active in investigations related to location and biometric data, utilizing Texas consumer protection laws, and the Texas DPSA may provide another tool for investigation and enforcement.

State attorneys general are also beginning to explore whether businesses are using artificial intelligence ("AI") systems in ways that violate privacy protections or fail to provide adequate transparency and consent mechanisms. In September 2024, an AI company in the health care industry entered into an Assurance of Voluntary Compliance ("AVC") with the Texas Attorney General in connection with alleged violations of the Texas Deceptive Trade Practices Act ("Texas DTPA"). Additionally, in February 2025, the Texas Attorney General's office opened an investigation of DeepSeek, a China-based AI company, for purported violations of Texas law.

With the confluence of state data privacy laws and the increasing use of AI in data processing and decision-making, companies that develop and use AI will likely need to address a range of privacy issues to meet their compliance goals. These may include how AI interacts with personal data and whether consumers are being properly informed about how their data is being used in AI systems. As AI continues to be a significant tool for businesses, privacy laws are likely to be significant tools state regulators use to examine the role of AI in data processing.

### *Wire Fraud and Business Email Compromise: An Evolving Role for Federal Law Enforcement*

A business email compromise, or "BEC," involves the manipulation or hijacking of corporate email systems to deceive employees into transferring funds to criminals. These incidents can involve impersonation of a vendor or known party, as discussed above, or even impersonation of an executive instructing a subordinate to wire money, often under the guise of urgency or confidentiality. The sophistication of these incidents has increased over time, with cybercriminals using social engineering tactics and technical methods to gain access to email accounts and conduct fraudulent wire transfers.

As noted above, in our experience, wire fraud related to BECs remains a major concern. Law enforcement agencies have had to evolve their strategies to address the growing threat posed by these crimes. Traditionally, the U.S. Secret Service has been tasked not only with protecting national leaders but also safeguarding the integrity of U.S. currency. However, as cybercrime has grown, so too has the Secret Service's role in protecting the nation's financial infrastructure. The agency has increasingly taken on the responsibility of investigating financial fraud cases, including wire fraud tied to BECs, and is focusing efforts on a proactive approach to email-based scams and wire fraud.

A key element in the Secret Service's evolving strategies to respond to cybercrime is its Global Investigative Operations Center ("GIOC"), which plays a pivotal role in helping to recover funds for victims of fraud, including BEC-related losses. The GIOC recently announced that it will focus efforts on cases involving more than $10,000 which are less than 30 days old. While it is still important to report all fraudulent transfers, this prioritization is a direct response to the growing sophistication and frequency of these crimes aimed at helping to ensure that law enforcement resources are well-positioned to intervene swiftly in high-value cases and increase the chances of recovering stolen funds.

Another aspect of the Secret Service's strategy has been an emphasis on collaboration. The Secret Service has partnered with local, state, and international agencies to share intelligence and resources. Working with the FBI, the Department of

Homeland Security, and other government agencies, as well as private sector firms, the Secret Service continues to build a collaborative network to be better equipped to tackle the complex nature of wire fraud and email compromise.

Additionally, the Secret Service has implemented public awareness campaigns aimed at educating businesses and individuals on the risks of BECs and wire fraud. These initiatives encourage better cybersecurity practices, which can reduce the likelihood of become a victim.

## Predictions for the Coming Year

### *State Enforcement Activity Will Increase*

State governments continue to be a driving force in privacy and compliance. The enactment of comprehensive state privacy laws provides another tool for investigations and enforcement. States may also follow suit with New York, which recently amended its data breach notification law to expand the definition of personal information to include additional data elements. These types of changes provide additional means for state regulators to investigate potentially unlawful activity and pursue enforcement actions to ensure compliance.

Even with the growing number of state privacy laws and the expanding scope of data breach notification requirements, companies can take proactive measures to protect themselves. Measures to prevent a data incident and comply with the regulations remain the best defenses against the growing risk of enforcement actions and penalties. Investments in robust compliance programs can help to mitigate the risk of potential violations and lessen or avoid costs associated with extensive regulatory scrutiny or penalties.

An initial step in the process is to develop comprehensive data privacy policies that align with applicable regulations, ensuring the guidelines are met. Regular audits of data handling processes–such as collection, storage, and processing–are also essential to ensure that practices align with those policies, as well as the applicable laws and regulations.

Additionally, since a significant number of compliance failures and data security incidents arise from human error, having a well-informed workforce that understands privacy obligations and data security best practices is crucial. Therefore, businesses should prioritize employee training and awareness.

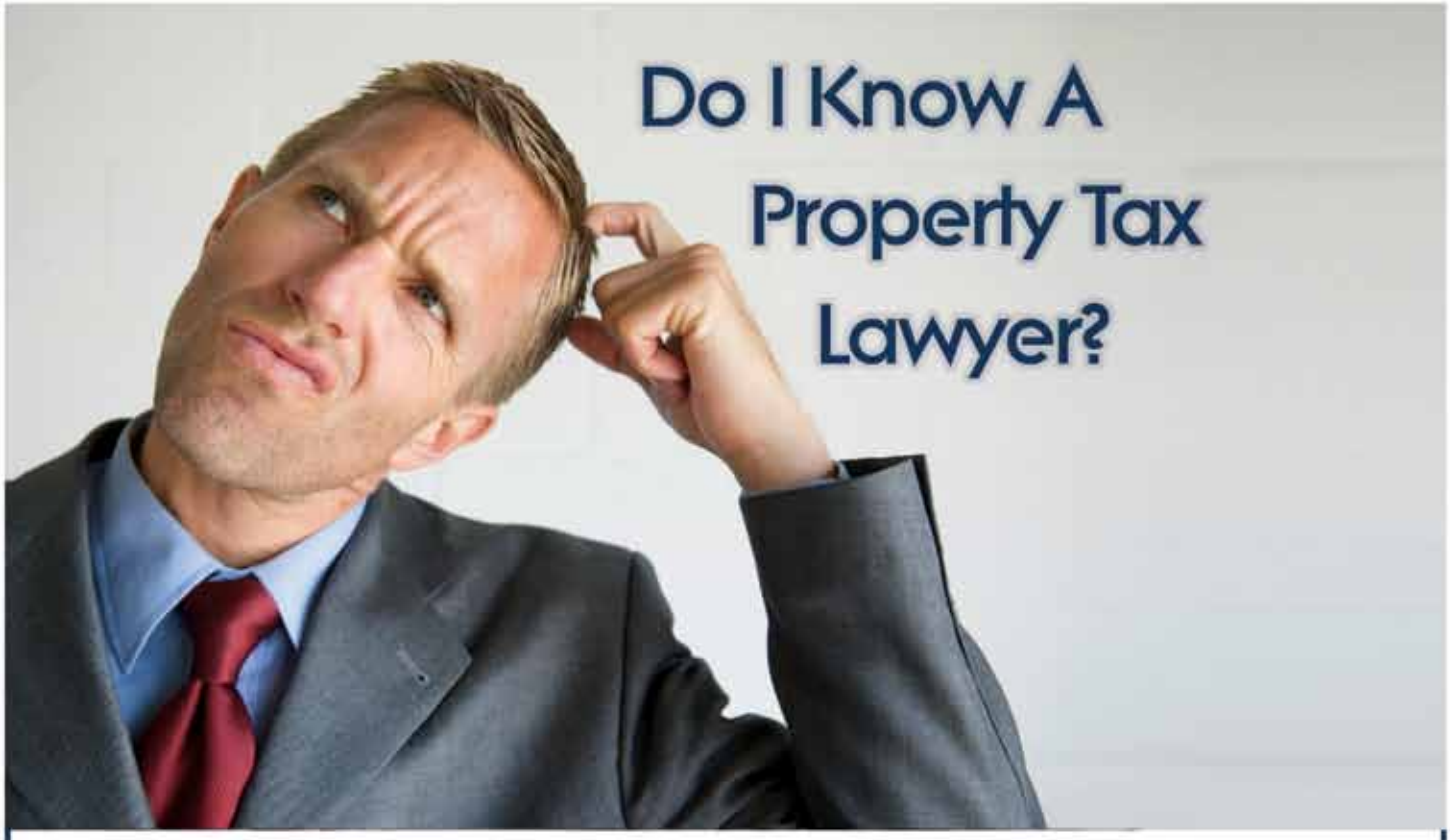
### *Phishing and Business Email Compromises Will Pervade*

As noted above, in many business email compromise events, the attacker phishes or socially engineers the victim to grant an unauthorized user to access their email account. That unauthorized user will often use the access to redirect a payment to an account under their control, to propagate more phishing emails to potential victims, or both. These types of attacks have been growing in recent years, and that trend could continue. These incidents are not as splashy as a headline-grabbing data leak on the dark web, or high-profile ransomware attack, but they can lead to financial loss and trigger notification obligations under state law.

While technical and policy measures such as MFA and voice verification procedures can help to mitigate threats, user vigilance is also a key tool for preventing phishing attacks. A strong awareness and training program that incorporates frequent testing and practicing what to do in the event of an incident can help users stay alert to these types of threats. Moreover, inculcating a culture that encourages users to report suspicious emails and self-report their own interaction with a potential phishing message can help to prevent or reduce the impact of a phishing attack.

### *AI in the Attacker Toolbox?*

AI has become a major topic of discussion in cybersecurity, with many speculating on its potential role in both defensive and offensive strategies. While AI is gaining traction, it continues to be a minor factor in the most common attack techniques today. Current attack strate-




BRUSNIAK TURNER

★★ PROPERTY TAX ATTORNEYS ★★

# COMPREHENSIVE STATEWIDE PROPERTY TAX REPRESENTATION

Trusted by Lawyers, Tax Consultants and Taxpayers Since 1981

17480 DALLAS PARKWAY, SUITE 210
DALLAS, TEXAS 75287
214.506.1073
JOHN@TEXASPROPERTYTAXATTORNEYS.COM

WWW.TEXASPROPERTYTAXATTORNEYS.COM

gies, such as phishing, social engineering, and exploiting known vulnerabilities, still dominate the landscape. Most threat actors rely on traditional tools and methods to execute their campaigns, and AI certainly has the potential to enhance attacks in the future. We anticipate seeing AI-powered chatbots used in social engineering or machine learning algorithms that can help identify vulnerabilities faster and more efficiently than traditional methods.

***Lynn Sessions*** *is a partner at BakerHostetler. Ms. Sessions leads the healthcare privacy and compliance team in the digital assets and data management practice group and serves as national co-lead of the healthcare industry team. She focuses her practice on healthcare privacy and data security, breach response, regulatory defense, and Health Insurance Portability and Accountability Act (HIPAA) compliance.*

***Kimi Gordy*** *is a partner at BakerHostetler. Ms. Gordy navigates complex cybersecurity and privacy issues for clients across the healthcare space. She is the firm's Houston digital assets and data management leader. Prior to joining BakerHostetler, she was a federal law clerk in the Southern District of Texas, giving her critical insight into the litigation risk that so often follows a data breach.*

***Pierce Cox*** *is an associate at BakerHostetler. He focuses his practice on digital risk advisory and cybersecurity, particularly in the areas of regulatory compliance, fraud investigation, and electronic discovery. He advises clients regarding compliance with data privacy laws, preparing for and reducing exposure to data privacy threats and mitigating potential losses from data breaches or misuse of information assets.*

***Jessica S. Johnson*** *is an associate at BakerHostetler. Her practice spans privacy and digital risk and cybersecurity, where she advises clients across various industries regarding compliance with federal, state, and international data security laws. Ms. Johnson guides clients across various industries through data security matters, including coordinating digital forensic investigations, determining breach notification obligations, and responding to regulatory inquiries.*

By LAURA L. FERGUSON

## NAVIGATING THE TEXAS DATA PRIVACY AND SECURITY ACT:

# Key Obligations and Implications for Businesses

Texas entered the state consumer privacy law fray over nine months ago when the Texas Data Privacy and Security Act ("TDPSA") went into effect.[1] This move was long-awaited and critical to protect the privacy and security of the vast amount of Texas residents' consumer data collected, processed, and shared by businesses every day, which consumer data is increasingly used for profiling or targeted advertising and presents a high risk to the consumer if the information were obtained by an unauthorized party.

### Application of the TDPSA

The TDPSA has one of the broadest reaches among state privacy laws, applying to any person that: (1) conducts business in Texas or produces a product or service consumed by Texas residents; (2) processes or engages in the "sale" of personal data; and (3) is not a small business as defined by the United States Small Business Administration ("SBA").[2] However, even small businesses are not fully exempt as the TDPSA restricts selling sensitive data without consumer consent. The TDPSA, like other state consumer privacy laws, does exempt financial institutions subject to Title V of the Gramm-Leach-Bliley Act, HIPAA-covered entities and businesses associates, state agencies and political subdivisions, certain nonprofit organizations, higher education institutions, and electric utilities, power generation companies, and retail electric providers.[3]

With respect to "small businesses," the TDPSA's exemptions track the SBA's categories, which are primarily based on the industry in which a business operates. The SBA has various industry-specific thresholds for a "small business" that typically vary by revenue (generally ranging from $2.25M to $47M) and/or number of employees (generally ranging from 100 to 1,500). While more than one of the North American Classification System Codes ("NAICS") may apply to a business, the business must self-identify the industry that is most applicable according to the size standard thresholds and continue to monitor for any changes over time.[4] Notably, the thresholds for qualifying as a small business under SBA standards are much more restrictive than the $25 million revenue thresholds employed by the consumer privacy laws in California[5] and Utah,[6] and, as a result, many more businesses fall under the TDPSA than under similar laws in other states.

### Obligations Under the TDPSA

For businesses that are not exempt, the TDPSA imposes obligations depending on the business' role as either a "controller" or "processor" of "personal data" of "consumers," with a heightened obligation for "sensitive data" and special rules for the "sale of personal data." These key terms are defined as follows:

- "Controller" means "an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data."
- "Processor" means "a person that processes personal data on behalf of a controller."
- "Personal data" means "any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual." Personal data does not include "deidentified data," publicly available information, or certain "pseudonymous data."

- "Consumer" means "an individual who is a resident of [Texas] acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context."[7]
- "Sensitive data" means "(A) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status; (B) genetic or biometric data that is processed for the purpose of uniquely identifying an individual; (C) personal data collected from a known child; or (D) precise geolocation data."
- "Sale of personal data" means "the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include: (A) the disclosure of personal data to a processor that processes the personal data on the controller's behalf; (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (C) the disclosure or transfer of personal data to an affiliate of the controller; (D) the disclosure of information that the consumer: (i) intentionally made available to the general public through a mass media channel; and (ii) did not restrict to a specific audience; or (E) the disclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition."

A controller is generally required to limit its collection of personal data to what is adequate, relevant, and reasonably necessary for the processing of the data as disclosed to the consumer; however, the controller can obtain the consumer's consent to avoid this restriction.[7] Even so, the controller is *required* to obtain the consumer's consent if it desires to collect sensitive data and further comply with the Children's Online Privacy Protection Act of 1998 if such data involves a known child.[8] The controller is prohibited from processing personal data in violation of state or federal consumer protection laws (prohibiting unlawful discrimination) and discriminating against a consumer for exercising their consumer rights. The controller must implement reasonable administrative, technical, and physical data security practices that are appropriate for the volume and nature of the personal data collected.

For controllers who engage in the processing of personal data for targeted advertising, selling personal data, processing data for purposes of profiling, processing sensitive data, or any processing activities involving personal data that represents a heightened risk of harm to consumers, the controller is required to conduct a fact-specific, written data protection assessment ("DPA").[9] The DPA must identify and weigh the potential benefits (both direct and indirect) and risks (taking into account mitigation safeguards) that may flow from the processing of such personal data to the controller, the consumer, other stakeholders, and the public.

Another key obligation of a controller is to provide a privacy notice to consumers that, among other requirements, details the categories of personal data collected, the purposes of processing such data, and how consumers can exercise their rights. Importantly, a controller that engages in the sale of sensitive or biometric data must also provide an explicit notice of such sale in the same manner and location as the privacy notice.[10] If the controller sells personal data to a third party for targeted advertising, the controller must provide information on the consumer's opt-out right and how to exercise it.

A processor, on the other hand, is required to adhere to the controller's instructions and assist the controller in meeting or complying with the controller's duties or requirements under the TDPSA, including assisting the controller

with responding to consumer requests, complying with breach reporting requirements, and providing information to help the controller conduct the DPA.[11] The controller-processor relationship must be governed by a contract that meets requirements specified in the TDPSA.

## Consumer Rights Under the TDPSA

Similar to other state consumer privacy laws enacted before the TDPSA, such as the California Consumer Privacy Act[12] and the Virginia Consumer Data Protection Act,[13] the TDPSA requires consumers have basic rights over their personal data, including the right to (1) confirm whether a controller is processing the consumer's personal data; (2) opt out of data processing for targeted advertising, sales of personal data, or profiling to inform certain decisions that will affect the consumer; (3) and access, correct, delete, and obtain a copy of the consumer's data. These consumer rights are immutable; the TDPSA prohibits any contract or agreement that purports to waive or limit these rights.[14]

When obtaining a consumer's consent for certain collection, processing, and selling of consumer data, the controller is required to obtain a written statement of the "consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer."[15] The consumer consent may be electronic, however a consent will not meet these requirements if the consumer merely (i) accepts general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (ii) hovers over, mutes, pauses, or closes a given piece of content; or (iii) agrees through the use of dark patterns (e.g., a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice).

## Enforcement of the TDPSA

There is no private right of action under the TDPSA. The Texas Attorney General has exclusive enforcement and investigative authority. As required by the TDPSA, the Texas Attorney General has posted information for consumers outlining their consumer rights and the responsibilities of controllers and processors under the TDPSA.[16] In addition, the Texas Attorney General established an online portal for consumers to submit complaints about a violation of their privacy rights or to report a data breach. As of the date of this article, the Texas Attorney General appears to have filed suit only against an auto insurance company for purported violations of the TDPSA;[17] however, the Texas Attorney General has expanded certain deceptive trade practices investigations into other businesses, such as car manufacturers, after the effective date of the TDPSA.[18]

> ***"There is no private right of action under the TDPSA. The Texas Attorney General has exclusive enforcement and investigative authority."***

Before bringing an enforcement action under the TDPSA, the Texas Attorney General must notify a person of an alleged violation, providing the person with a 30-day cure period to resolve the violation and provide the Texas Attorney General with a written statement that shows that the (i) violation was corrected (and provides proof of same), (ii) consumer was notified of such correction (if the person has the consumer's contact information), and (iii) confirms internal policies have been modified as necessary to prevent future violations. If a violation is not timely cured or the written statement to the Texas Attorney General is violated, the offending person may face civil penalties (up to $7,500 for each ⁅violation⁆ and injunctive relief (to restrain or enjoin the person's operations), as well as potential liability for the Texas Attorney General's reasonable attorney's fees and other enforcement-related expenses.

The TDPSA marks a pivotal advancement in safeguarding consumer data privacy and security for Texas. With its broad reach, the TDPSA imposes stringent requirements on a wide array of businesses, including those that may not meet the applicability thresholds in other states. Businesses operating in Texas or serving Texas residents must diligently adhere to the TDPSA's comprehensive mandates, from understanding the roles and obligations of controllers and processors to implementing robust data protection measures and respecting consumer rights. By doing so, businesses can mitigate risks, avoid penalties, and build trust with their customers. As enforcement of the TDPSA continues to evolve, staying informed and proactive in compliance efforts will be crucial for businesses to avoid penalties and maintain a strong reputation in the ever-growing Texas marketplace.

***Laura L. Ferguson*** *is a partner in the Houston office of Troutman Pepper Locke LLP, specializing in privacy and cybersecurity, as well as employee benefits and executive compensation.*

## Endnotes

1. TEX. BUS. & COM. CODE §§ 541.001 et. seq.
2. *Id.* § 541.002(a).
3. *Id.* § 541.002(b).
4. *See* U.S. Small Business Administration, Table of Size Standards,https://www.sba.godocument/support-table-size-standards (last visited March 23, 2025).
5. CAL. CIV. CODE §§ 1798.100–1798.199.100.
6. UTAH CODE § 13-61-101 et seq.
7. TEX. BUS. & COM. CODE § 541.101.
8. 15 U.S.C. § 6501 et seq.
9. TEX. BUS. & COM. CODE § 541.105.
10. *Id.* § 541.102.
11. *Id.* § 541.104(a).
12. CAL. CIV. CODE §§ 1798.100 - 1798.199.100.
13. VIRGINIA CODE §§ 59.1-575 through 59.1-585.
14. TEX. BUS. & COM. CODE § 541.054.
15. *Id.* § 541.001(6).
16. *See* https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/texas-data-privacy-and-security-act (last visited March 23, 2025).
17. *See* Texas Attorney General press release: https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45 (last visited March 23, 2025).
18. *See* https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-general-motors-unlawfully-collecting-drivers-private-data-and (last visited March 23, 2025) and https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-opens-investigation-car-manufacturers-collection-and-sale-drivers-data (last visited March 23, 2025).

JAMS WELCOMES

# Marie R. Yeates, Esq.


Ms. Yeates became widely recognized as one of the nation's foremost appellate attorneys during her illustrious 43-year career at Vinson & Elkins. She argued 141 appellate cases before federal and state courts nationwide and played a key role in landmark appellate victories. She has been consistently recognized in *Chambers USA* since 2003, earning the distinction of "Senior Statespeople" in 2024. At JAMS, she will serve as a mediator, arbitrator, referee/special master and neutral evaluator in **appellate, business/commercial, construction, energy & utilities, environmental, maritime & admiralty** and **personal injury** matters. Visit **jamsadr.com/yeates** or scan the QR code to learn more.

JAMS®

By INNOVATIVE DRIVEN (ID)

# The Importance of Data Privacy and Security for Law Firms

In an era of escalating cyber threats, data privacy and security are critical concerns for law firms. The legal industry handles extensive amounts of sensitive information, making it an inviting target for cybercriminals. In 2024, the rising number of breaches spotlighted the need for all-sized firms to adopt strong cybersecurity measures to protect client confidentiality and maintain trust.

## The Breach Landscape: Real World Impacts

According to IBM's Cost of a Data Breach Report,[1] the global average cost of a data breach in 2024 reached an all-time high of $4.88 million, reflecting a 10% increase from the previous year. The financial repercussions of a data breach can be even more painful for law firms. Two recent examples highlight the growing risks, with one firm agreeing to an $8.5 million settlement over a 2022 data breach that exposed thousands of individuals' personal and health information, while a second firm reached an $8 million settlement in April 2024 after a breach compromised the personal data of more than 600,000 people.

Beyond the financial and potential reputational brand damage, data breaches can impact firms on several other fronts. Phil Favro,[2] a court-appointed special master and expert advisor, highlights several considerations:

***Litigation***. Firms are in the business of generating income by representing client interests. When firms shift to a defensive posture to address harm arising from a data breach, income-generating resources are redirected to protecting firm interests. This means firms may have to (among other things) address the concerns of government regulators and litigate to defend firm interests against impacted parties, both draining firm resources and revenue.

***Ethics***. It is not a stretch to suggest that data breaches could result in lawyers being disciplined under certain circumstances. This is particularly the case where firms have not taken reasonable steps to prevent inadvertent disclosures of client information.[3] Professional discipline can severely impact a lawyer's reputation, ability to practice law, and future earnings.

## In the Crosshairs: Measures for Security

Law firms hold valuable data, from confidential client communications to personally identifiable information (PII) and health records. Cybercriminals target firms with outdated security measures, making them vulnerable to attacks. By adopting several defensive and offensive measures, they can reduce risk and increase firm and client data security.

***Multifactor Authentication (MFA)***: The American Bar Association's 2023 Cybersecurity TechReport survey found that only 54% of attorneys had MFA available, despite Microsoft reporting that MFA can block 99.9% of credential-based attacks. Enforcing MFA across all platforms is a fundamental step toward improved security.[4]

***Software Updates and Patch Management***: Another American Bar Association study found that 42% of law firms with 100 or more employees were using outdated software.[5] Regular updates and patching are essential to closing security gaps.

Jason Brandes,[6] an executive with 25+ years of experience in data management, offers a proactive perspective, noting that data compliance and data management are crucial for data privacy and security because they ensure that organizations handle data responsibly, legally, and efficiently.

***Data Compliance***: Ensures adherence to regulations (*e.g.*, GDPR, CCPA) to protect sensitive information, reduce legal risks, and maintain customer trust.

***Data Management***: Enforces policies, controls, and best practices for data storage, access, and lifecycle management, minimizing risks of breaches and unauthorized access.

### Generative AI: Balancing Innovation With Data Privacy and Security

Law firms are increasingly turning to generative AI (GenAI) to enhance efficiency and improve legal research. However, these tools pose data privacy risks to manage. Cathy Fetgatter,[7] senior vice president of analytics & managed review at Innovative Driven, and Wayland Radin,[8] VP of analytics, weigh in below with their team's perspective.

GenAI models are initially trained on vast amounts of publicly available and user-provided data—sometimes "memorizing" sensitive inputs. This raises concerns about the inadvertent disclosure and improper use of confidential client information. The release of ChatGPT in late 2022 marked a turning point in GenAI adoption, making advanced language models widely accessible for the first time. However, many users fail to realize that these tools often still learn from their interactions. The familiar thumbs-up/thumbs-down feedback buttons on platforms like ChatGPT serve as a reminder that user interactions continue to refine these models. In some cases, even without explicit feedback, AI providers may collect data to improve their systems—reinforcing the adage used by Google, Facebook, and other tech companies: "If you're not paying for the product, you are the product."

GenAI providers, particularly consumer-facing ones, rely on user inputs to train their models, and some monetize data by selling insights or sharing information with third parties. If an AI tool does not explicitly guarantee confidentiality, anything inputted—such as privileged communications, personally identifiable information (PII), or sensitive health data—may become part of a broader dataset with unintended exposure. To mitigate these risks, law firms should adopt a cautious approach:

***Review Terms of Service***: Before integrating any GenAI tool, firms must understand its privacy policies and security commitments.

***Control Prompt Data***: Users should avoid entering sensitive or privileged data unless they are certain the tool enforces strict confidentiality measures. Many firms bring these tools wholly in-house for this reason.

***Manage Data Retention***: Many AI tools store prompt histories by default. Firms should consider disabling retention settings or ensuring data deletion after each session.

The convenience and power of GenAI come with significant responsibilities, particularly in the legal industry where confidentiality is paramount. While these tools can enhance efficiency, law firms must remain vigilant, ensuring that the benefits of AI do not come at the cost of ethical obligations nor client trust. By establishing clear protocols and carefully vetting AI tools, firms can harness AI's potential while safeguarding the integrity of their data.

### Conclusion

With cyber threats showing no signs of slowing, law firms must take decisive action to protect client data. By implementing defensive and offensive measures, ensuring strong information governance, and addressing the unique challenges of GenAI, firms can mitigate risks and uphold their commitment to client confidentiality. In today's evolving technology landscape, proactive cybersecurity is essential.



### Endnotes

1. *Cost of a Data Breach Report 2024*, IBM, https://www.ibm.com/reports/data-breach (last visited Mar. 21, 2025).
2. Philip Favro, LINKEDIN, https://www.linkedin.com/in/philip-favro-b1a27ba/ (last visited Mar. 21, 2025 11:02 AM).
3. *See* MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N 1983).
4. John Simek, *2023 Cybersecurity TechReport*, AM. BAR ASS'N (Dec. 18, 2023), https://www.americanbar.org/groups/law_practice/resources/tech-report/2023/2023-cybersecurity-techreport/.
5. Dan Roe, *Law Firm Data Breach Reports Show No Signs of Slowing in 2024*, THE AM. LAW. (May 23, 2024 5:00 AM), https://www.law.com/americanlawyer/2024/05/23/law-firm-data-breach-reports-show-no-signs-of-slowing-in-2024/?slreturn=20250319-12254.
6. Jason Brandes, LINKEDIN, https://www.linkedin.com/in/jason-brandes-81411622/ (last visited Mar. 21, 2025 11:05 AM).
7. Cathy A. Fetgatter, LINKEDIN, https://www.linkedin.com/in/cathy-a-fetgatter-22263b8/ (last visited Mar. 21, 2025 11:06 AM).
8. Wayland Radin, LINKEDIN, https://www.linkedin.com/in/wayland-radin/ (last visited Mar. 21, 2025 11:07 AM).


By ERIC BENAVIDES

## THE HARRIS COUNTY RIC COURT:

# Paving the Way for Rehabilitation and Change

The Harris County Responsive Interventions for Change Docket, commonly known as the RIC Court, represents a progressive approach to criminal justice that seeks to address the root causes of criminal behavior and to foster rehabilitation. Since being established, the RIC Court has joined an innovative set of specialty courts designed to offer an alternative to traditional punitive measures. By focusing on rehabilitation and individualized treatment plans, the RIC Court has been instrumental in attempts to reduce recidivism, improve public safety, and help individuals regain control over their lives.

### The Genesis of the RIC Court

The RIC Court was created as a response to the growing need for alternatives to incarceration, particularly for individuals whose criminal behavior is closely linked to underlying issues, such as mental illness, substance use, or trauma. The traditional criminal justice system often fails to address these root causes and, as a result, individuals may cycle in and out of jail or prison without experiencing long-term improvements in their behavior. In response, the RIC Court was created to implement a model that would provide comprehensive support and services to these individuals, while holding them accountable for their actions.

The RIC Court's creation aligns with the broader movement across the United States, which has seen a rise in specialty courts, such as drug courts, mental health courts, and veteran courts. These courts aim to provide tailored interventions that target the specific challenges certain defendants face, offering them a chance for recovery, personal growth, and reintegration into society.

### The Structure and Operation of the RIC Court

The two types of potential outcomes in RIC Court are Pre-Trial Interventions or Deferred Adjudication. Based on the results of an interview and assessment, the programs may include drug treatment, community service, and any other courses that may be deemed appropriate on a case-by-case basis.

A Pre-Trial Intervention is available to those with little to no criminal history. It is a better option for defendants as there is no plea of guilt. The program is typically one year long and takes place while the case is still active and pending. Upon successful completion of the program, the defendant will receive a full dismissal and be eligible for an expunction.

A Deferred Adjudication is more likely for those with a more extensive criminal history, or with repeat referrals to the RIC Court. A Deferred Adjudication differs from Pre-Trial Intervention in that defendants do plead guilty; however, a finding of guilt is deferred until after a probation period. If the individual successfully completes probation, there will not be a final conviction. However, he or she is not eligible for an expunction but is eligible for a "non-disclosure," which is a partial sealing of the record.

### Plea Mill?

The RIC Court has faced criticism for

being a "plea mill," with some arguing that it encourages defendants to quickly accept plea deals rather than fully contest their charges. Critics contend that this system pressures individuals into quickly agreeing to pleas, sometimes without fully exploring the merits of their cases. However, defendants still retain their constitutional right to due process throughout the adjudicative process. Defendants can always challenge the charges against them, present a defense, and fight their case in court. But if a defendant decides to contest the charges or refuses the treatment or plea deal offered in RIC Court, their case will be sent back to their home court, where they can proceed with a more traditional legal process. This ensures that every individual still has access to a fair trial if they choose that route.

> *"A Pre-Trial Intervention is available to those with little to no criminal history. It is a better option for defendants as there is no plea of guilt."*

## The Short- and Long-Term Impact of the RIC Court

The RIC Court has proven to be more cost effective than traditional incarceration. Studies have shown that specialized courts like the RIC Court can reduce the costs associated with jails and prisons, while also improving public safety. Rather than incurring the high costs of incarceration, the RIC Court prioritizes rehabilitation programs that are more affordable and effective in the long run. Participants in the RIC Court must also pay fees through their programs, which can bring money in instead of having money go out.

More time is needed to see if the RIC Court truly helps with the rate of recidivism, but at a minimum, it gives each defendant an opportunity to make a personal decision about their lives—something that a jail or prison would never provide.

The Harris County RIC Court stands as a model for innovation in the criminal justice system. As the court continues to evolve and grow, it offers a unique opportunity to assist in breaking the cycle of generational incarceration.

***Eric Benavides*** *is a highly experienced Houston criminal defense attorney, with over 1,000 case dismissals and multiple not guilty verdicts to his name. As the founder and head of Benavides Law Group, he has been recognized as a Texas Super Lawyer for his exceptional legal skills and commitment to defending his clients.*

# Houston Bar Association's Charitable 8K Race Rings in Milestone

For 40 years, the HBA Eikenburg Fun Run has brought Houston's legal community (and the public) together as a charity race benefiting Pursuit Center. The Houston nonprofit—commemorating its 75th anniversary this year—serves individuals with intellectual and developmental disabilities and autism. This year's event welcomed hundreds of runners to Sam Houston Park in downtown Houston on February 15, featuring the popular 8K portion of the event and the 1-mile family walk.

The race is named in honor of the late HBA Past President John J. Eikenburg, who created the event during his Bar Year (1985-1986). Upon Mr. Eikenburg's passing in 1997, the HBA Board of Directors voted to rename the run in his honor. His son, John J. Eikenburg, Jr., participates with his family nearly every year.

Special thanks to the co-chairs of this year's Fun Run Committee: Rick Anderson, Husch Blackwell LLP; Maine Goodfellow, Phillips 66; and Adam Weaver, Pillsbury Winthrop Shaw Pittman LLP. The HBA also thanks Harris County Precinct One Constable Alan Rosen for his long-time support of the Fun Run.

*Photos by Anthony Rathbun Photography*

## CONGRATULATIONS TO THIS YEAR'S WINNERS

**President's Trophy**

*(Awarded to fastest Houston legal team with at least 1 attorney):*

**Clark Hill Houston Striders Connection**
*Firm*: Clark Hill; *Runners*: **Hayden Lightfoot, Mark Speets, John Spiller**.

**Seymour Lieberman Law School Team Trophy**

*(awarded to the fastest law student team)*

**Legally Fast** – *Law School*: South Texas College of Law Houston; *Sponsor*: Anne & Done Fizer Foundation; Runners: **Jonathan Andrew, Ethan Gant, and Caleb Ortega**.

**Men's Open**

**Clark Hill Houston Striders Connection**

**Women's Open**

**Damas y Demandas** – *Law School*: South Texas College of Law Houston; *Sponsor*: Jenkins & Kamin, LLP; *Runners*: **Laura Garza, Julia Ramos, Kathleen Sandoval**.

**Open Mixed**

**Space City Striders – Alvin Adjei, Terence Baptiste, Sam Torres**.

**Mixed Masters**

**Hispanic Bar Association – Cindy Peters, Dirk Peters, Daniel Rodriguez**.

*See the full list of this year's winners at hba.org/funrun.*

**Overall Male Open**
**Valentino Julien**

**Overall Female Open**
**Carli Langley**

**Overall Male Masters**
**David Alber**

**Overall Female Masters**
**Heidi Zimmerman**

**Overall Male Veterans**
**Chris Robbins**

**Overall Female Veterans**
**Allyson Serrao**

Mark Speets (L) and Hayden Lightfoot with the Clark Hill Houston Striders. The team placed first in the Men's Open and took home the President's Trophy. (Not photographed: John Spiller).

Chris Robbins (L) and Allyson Serrao, winners of the veterans categories.

The Space City Striders (L to R) Alvin Adjei, Sam Torres, and Terence Baptiste), first place winners of the Open Mixed category.

Heidi Zimmerman, winner of the Overall Female Masters category.

Current and past chairs of the HBA Fun Run Committee. (L to R) Rick Anderson ('25), Lawrence Winsor ('23), Benjamin Roberts ('23 & '24), Amber Morrison ('21 & '22), Adam Weaver ('24 & '25), Maine Goodfellow ('23 & '24), Nico Zulli ('22), Alistair Dawson ('15), Susan Oehl ('15 & '16), Todd Frankfort ('00), Cassandra McGarvey ('17 & '18), John Spiller ('11), David M. Ratchford ('02), Dora (Martinez) Patout ('09), Cara Vasquez ('21).

Valentino Julien, Overall Male Open winner.

HOUSTON BAR FOUNDATION

HBF

EST. 1982

# BECOME AN HBF FELLOW

**LEARN MORE AT HBA.ORG/FELLOWS**

**DID YOU KNOW?**

**HBA MEMBERS ARE AUTOMATICALLY MEMBERS OF THE HOUSTON BAR FOUNDATION BUT NOT AUTOMATICALLY FELLOWS.**

**REQUEST A NOMINATION TO BECOME AN HBF FELLOW TODAY!**

## Our Mission

The Houston Bar Foundation's mission, as the charitable arm of the HBA, is to make a positive impact on our community by:
- supporting legal representation for those in need,
- promoting understanding of our legal system, and
- fostering the administration of justice.

***Strengthen your Houston community and charitable support***

Fellow Categories:
- Fellow
- Life Fellow
- Sustaining Life Fellow
- Champion Fellow (NEW)

**Interested in becoming an HBF Fellow?**
**Wish to submit a Fellow's nomination?**
**Ready to upgrade your Fellowship level?**

**Contact Ron Riojas at ronr@hba.org.**

Fellows make a $2,500 charitable contribution that can be paid:
- upon appointment,
- monthly, or
- annually.

Only HBA members are eligible to become a Fellow.

John J. Eikenburg, Jr.

South Texas College of Law Houston's *Legally Fast* student team took home the Seymour Lieberman Law School Team Trophy. They were sponsored by the Anne and Don Fizer Foundation. (L to R) Caleb Ortega, Ethan Gant, and Jonathan Andrew.

HBA President-Elect Daniella Landers (L) with HBA Board Member Sam Torres.

## THANK YOU TO THE 2025 HBA FUN RUN SPONSORS

### PLATINUM

### GOLD

### SILVER

### BRONZE

ADR of Counsel Mediators • BWA Video, Inc. • Clark Hill • Duane Morris LLP • Maine Goodfellow • HBA Family Law Section • HBA Real Estate Section • HisBA/MABAH • Houston Lawyer Referral Service
Jackson Walker LLP • Oweyssi Law Firm • Shook Hardy Bacon • Veritas Research, LP • Weil, Gotshal & Manges LLP • Adam & Casey Weaver • Lawrence & Erica Winsor • Zach Wolfe Law Firm

### FRIENDS & SUPPORTERS

Todd Lonergan • Stephanie Noble

## THANK YOU TO THE FOLLOWING FOR THEIR SUPPORT

*Beer donated by:* **Equal Parts Brewing**
*Drink Hydration Mix donated by:*
**Skratch Labs**
*Water donated by:* **Watermill Express**
*Breakfast Tacos donated by:*
**HisBA and MABAH**
*Bagels donated by:* **The Hot Bagel Shop**
*Fruit & Drinks donated by:* **Todd Lonergan**
*Salads donated by:* **Salata**
*Volunteers provided by:*
**The Houston Astros Foundation**
*Music provided by:* **Grand Old Grizzly**
*Entertainment provided by:*
**Cheerful Clowns**
*Pre-race stretches provided by:*
**Bloom Fitness**

**Door prizes donated by:**
**Pursuit Center**
**Little Matt's**
**Postino**
**The Buffalo Grill**
**Irina Tsveklova**

# Houston Bar Foundation Celebrates Achievements and Lays Groundwork for Year Ahead at 2025 Annual Luncheon

Sara Keith, senior legal counsel with Shell USA, Inc., assumed the role of 2025 Houston Bar Foundation Chair at the Foundation's Annual Luncheon on February 13. Keith succeeds Linda Hester. Under Hester's leadership, the Foundation revised its mission statement; updated its Fellows Program, including introducing an exciting new Fellows category called "Champion Fellows"—recognizing Fellows who provide substantial long-term support for the HBF's access to justice and high-impact programming; and established the HBF Community Grants Program, which will provide grants to qualified local projects that align with the mission of the Foundation. (Learn more about the Foundation's work and how Fellows play a vital role to support the HBF's charitable programs and recipients in the greater Houston area at ***hba.org/foundation***.)

2024 HBF Chair Linda Hester (R) presents the 2025 James B. Sales Pro Bono Leadership Award to Denise Scofield.

"I am incredibly honored to serve as the 2025 Chair of the Houston Bar Foundation. I am proud of everything the Foundation has accomplished this year to broaden and deepen the impact of our work to improve the lives of our fellow Houstonians," said Keith. "Our accomplishments are possible because of our dedicated board, HBA staff, the generosity of our fellows, and our amazing Houston legal community. I am grateful to Linda for her dedicated leadership, service, and stewardship of the Foundation during her term as Chair. I look forward to serving at the helm of the Foundation and working with our Board of Directors to continue championing programs that support access to justice in the greater Houston area."

Keith is an accomplished litigator and bankruptcy lawyer with over 16 years of experience. She joined Shell USA, Inc. in December 2018, where she advises executive leadership and key stakeholders on insolvency matters, litigation, commercial credit negotiations, risk management, and compliance. In addition to serving as the HBF Chair, Keith is International Women's Insolvency & Restructuring Confederation (IWIRC)–Houston Network president, Shell Women Adding Value Everywhere (WAVE) Woodcreek Chapter vice president, an HBF Fellow, and a Texas Bar Foundation fellow. She is also the 2025 Shell U.S. Legal Pro Bono & Community Service Program Veterans Clinic co-lead and serves on numerous planning committees for several Texas legal conferences.

The Foundation's board includes 2023-2025 directors Andrew Edelman of LyondellBasell, Holly Chastain Nini of CITGO Petroleum Corp., and Christopher D. Northcutt of Chevron Corporation; 2024-2026 directors Benny Agosto, Jr. of Abraham, Watkins, Nichols, Agosto, Aziz & Stogner; Jennifer A. Hasley of Hasley Scarano, L.L.P.; Stephanie Noble, Vinson & Elkins LLP; and Krisina Zuñiga, Susman Godfrey L.L.P.; and incoming 2025-2027 directors Sejal Brahmbhatt of Williams Hart & Boundas, LLP; Hon. Mike Engelhart of Kherkher Garcia, LLP; former HBA Executive Director Mindy Davidson; and Denise Scofield of O'Melveny & Myers LLP. Linda Hester will serve on the board as Immediate Past Chair. HBA President David Harrell of Troutman Pepper Locke LLP will serve as Ex Officio, as will HBA Executive Director and Secretary of the HBF Board Vinh Ho.

Judge Sofía Adrogué, an inaugural judge of the newly-established Eleventh Business Court Division, delivered the luncheon's keynote address. In her remarks, Judge Adrogué spoke about the pressing need for pro bono legal services in the greater Houston community.

The Foundation also presented the 2025 James B. Sales Pro Bono Leadership Award to Denise Scofield. The award, established in 2009, recognizes the excellence that has been the hallmark of the Foundation's leadership.

Over the past three decades, Scofield has spent significant time representing low-income individuals on a pro bono basis on a wide array of issues, including domestic violence, contested divorce and custody, and disability rights. She has served locally and statewide in leadership positions to address the justice gap in Texas. Here in Houston, Scofield served on, and chaired, the Houston Volunteer Lawyers board, then led fundraising efforts that raised hundreds of thousands of dollars for HVL as a president of the Houston Bar Association and chair of the Houston Bar Foundation. She is a long-time director of the Texas Access to Justice Foundation and regularly advocates for funding and support of legal aid.

Additional awards presented at the luncheon were the Houston Volunteer Lawyers (HVL) Pro Bono Awards, as well as recipients of awards from the Harris County Dispute Resolution Center (DRC) and *The Houston Lawyer* magazine. Additional information about the awards can be found at ***hba.org/foundation***.

*Photos by Deborah Wallace, Barfield Photography*

The 2024 HBF Board of Directors. (L to R) Vinh Ho, Jennifer A. Hasley, Stephanie Noble, Sejal Brahmbhatt, Sara Keith, Linda Hester, Alistair Dawson, Holly Chastain Nini, Andrew Edelman, and Christopher D. Northcutt. (Not pictured: Benny Agosto, Jr.; Diana Gomez; Monica Karuturi; Richard Whiteley; and Krisina Zuñiga.)

(L to R) HBA President David Harrell with Judge Sofia Adrogué and Judge Grant Dorfman of the Texas Business Court Eleventh Division.

2025 HBF Chair Sara Keith (R) presented Immediate Past Chair Linda Hester with a plaque recognizing Hester's leadership, stewardship, and dedication to the Foundation.

The 2025 HBF Board of Directors (L to R) Vinh Ho, Jennifer A. Hasley, Stephanie Noble, Sejal Brahmbhatt, Hon. Mike Engelhart, Sara Keith, Mindy Davidson, Andrew Edelman, Christopher D. Northcutt, Linda Hester, Holly Chastain Nini, and Denise Scofield. (Not pictured: Benny Agosto, Jr.; David Harrell; and Krisina Zuñiga.)

## 2025 HVL Pro Bono Award Winners

Baker Hughes was this year's recipient of the Corporate Law Department Award. Accepting on their behalf was (L to R) Timothy Morella, Victor Wright, Gabriela Espinoza, Maria Guadalupe Carreon, Ivett Hughes, Benjamin Leibman, Mathew Sampson, Benjamin Weber, and Marta Pajaro.

***HVL Pro Bono Award Winners Not Photographed***

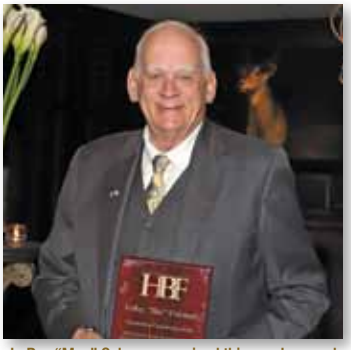
**Large Law Firm**
Kirkland & Ellis LLP

**Mid-Size Law Firm**
Shook, Hardy & Bacon L.L.P.

**Individual**
Shay Johanson

Jenkins & Kamin, LLP received this year's award for Small Law Firm. (L to R) Melissa Cass Pickett, Lauren L. Heyde, Elva Godwin, Aaron M. Reimer, Lynn Kamin, Peter F. Walbridge, Jr., Claudia M. Canales, Susan E. Oehl, and Jeanice Dawes.

## Dispute Resolution Center Award Winners



LeRoy "Mac" Coleman received this year's award for Outstanding Contribution to the DRC.

Stanley Santire was recognized for Longevity of Service to the DRC.

## *The Houston Lawyer* Outstanding Legal Article

Dave Louie, lead counsel with LyondellBasell and member of *The Houston Lawyer* editorial board, is the recipient of this year's award in recognition of his article, "The Many Titles of Tasha Schwikert Moser" from the January/February 2024 issue.

# Equal Access Champions

The firms and corporations listed below have agreed to assume a leadership role in providing equal access to justice for all Harris County citizens. Each has made a commitment to provide representation in a certain number of cases through the Houston Volunteers Lawyers.

Abraham, Watkins, Nichols, Agosto, Aziz & Stogner
Akin Gump Strauss Hauer & Feld LLP
Angela Solice, Attorney at Law
Archie Law PLLC
Baker Botts L.L.P.
BakerHostetler LLP
Baker Hughes
Beck Redden LLP
Blank Rome LLP
Bracewell LLP
CenterPoint Energy, Inc.
Chamberlain Hrdlicka
Chevron USA
Coane & Associates
Dentons US LLP
Elizabeth S. Pagel, PLLC
Eversheds Sutherland US LLP
Exxon Mobil Corporation
Fleurinord Law PLLC
Foley & Lardner LLP
Fuqua & Associates, P.C.
Gibbs & Bruns LLP
Gibson, Dunn & Crutcher LLP
Gray Reed
Greenberg Traurig, LLP
Halliburton
Hasley Scarano, L.L.P.
Haynes and Boone, LLP
Hunton Andrews Kurth LLP
Jackson Walker LLP
Jenkins & Kamin, L.L.P.
King & Spalding LLP
Kirkland & Ellis LLP
Law Office of Cindi L. Rickman
Law Office of Norma Levine Trusch
Law Offices of Omonzusi Imobioh
Limbaga Law
LyondellBasell Industries
Martin R.G. Marasigan Law Offices
McDowell & Hetherington LLP
McGarvey PLLC
Morgan, Lewis & Bockius LLP
Northum Law
Norton Rose Fulbright
O'Melveny & Myers LLP
Painter Law Firm PLLC
Reed Smith LLP
Royston, Rayzor, Vickery & Williams, LLP
Sanchez Law Firm
Shell USA, Inc.
Shipley Snell Montgomery LLP
Shortt & Nguyen, P.C.
Sidley Austin LLP
Sorrels Law
Squire Patton Boggs
The Ericksen Law Firm
The Jurek Law Group, PLLC
Troutman Pepper Locke LLP
Vasquez Waite
Vinson & Elkins LLP
Weycer, Kaplan, Pulaski & Zuber, P.C.
Wilson, Cribbs, & Goren, P.C.
Winstead PC
Winston & Strawn LLP
Yetter Coleman LLP

# A Journey to Top of the World with David Barron

**By CAREY WORRELL**

David Barron is a Houston lawyer through and through, having earned undergraduate and law degrees from the University of Houston. With almost 30 years of experience, David is a seasoned labor and employment lawyer with Cozen O'Connor. While negotiating collective bargaining agreements and winning courtroom battles regarding discrimination, trade secret theft, and non-competition agreements, those stories do not compare to Barron's description of his hiking adventures around the world, including a trek to Everest base camp.

Barron in Kathmandu.

The plans for Barron's trip to Everest Base Camp really started in his son's boy scout troop. Prior to getting involved in scouting, Barron had not done much hiking and adventuring, but he met people in that group who inspired him and his son to expand their horizons. Since Barron started adventuring, he has not stopped. He has climbed Guadalupe Peak (the tallest mountain in Texas) during snowy conditions, hiked the Grand Canyon, rim-to-rim in ONE DAY, and used summiting the 14,000-foot Pikes Peak as a training climb for his trip to Everest.


Barron (far right) at Pikes Peak Summit.

According to Barron, getting to base camp is not an easy undertaking. It starts with a flight to Kathmandu and a stay at the famed Yak and Yeti Hotel. The next leg of the trip involved a helicopter trip to Lukla, home of the world's "most dangerous airport." The Tenzing-Hillary Airport in Lukla has an incredibly short runway that only allows helicopters or planes known as STOL (short take-off and landing) aircraft. After surviving the helicopter landing in Lukla (considered much safer than landing in an airplane), Barron, along with six other people, including two Sherpa guides and additional people to carry all the gear, started the week-long trek to Base Camp. On his way to Base Camp, Barron passed through the Sherpa capital of Namche Bazaar, experienced a blizzard that forced his group to change their route, and suffered the physical challenges of spending time at such high altitude. Getting to Base Camp requires a slow pace so that everyone can acclimate to the altitude by stopping at a series of tea houses (similar to a very basic hotel) along the way.

Barron in Gokyo.

Upon arrival at Base Camp, Barron walked through an area dedicated to memorializing all of the adventurers who have died on Mount Everest from all over the world. This humbling experience may have something to do with Barron's response when I asked him if he has plans to attempt an Everest summit in the future. This lawyer, who has completed many marathons, several 100-mile races, a Spartan Ultra 50K and the Brazos Bend 50K, unequivocally stated: "No, that would he a whole other level."

***Carey Worrell** is the managing attorney of SimpleLawTX, a Texas law firm specializing in offering efficient solutions in the areas of business, real estate, estate planning, probate, and immigration. She is a member of* The Houston Lawyer *editorial board.*

# A Profile
## IN PROFESSIONALISM

**LAURA GIBSON**
Office Managing Partner, Dentons US LLP
HBA Past President (2015-2016)

My father, David Gibson, was a great lawyer. Triple board certified in family law, criminal law, and civil trial law, he practiced from 1957 until shortly before his death from cancer in 1990 at the age of 56. Before he passed away, the Gulf Coast Family Law Specialists presented an award in his honor named the David A. Gibson Award for Excellence and Professionalism. Even though I never worked as a lawyer for my dad, I learned the foundation of what makes a good lawyer from him. From my experience after his death, I also learned the importance of planning for the inevitable cessation of practice.

My dad taught me that a lawyer's word is his bond. He made me understand that a lawyer wants her opposing counsel to be as qualified as possible. He stressed that we have a duty to present the facts in the best light to our client, but that we don't make the facts, nor should we try to. He emphasized that our job is not to win at all costs, but to ensure justice is served.

When my father passed away, he was a solo practitioner and did not have a custodian attorney. That responsibility fell on me. I was a four-and-a-half-year associate at what is now Troutman Pepper Locke.

The number of lawyers who are dying, becoming disabled, or disappearing without taking steps to close their practices is increasing. This critical problem will only grow worse unless we work to promptly address it.

I had the privilege of serving as the president of the State Bar of Texas from 2022-2023. My primary initiative during my presidency was to work to promote succession planning to encourage solo practitioner lawyers to designate a custodian attorney.

We have heard of the "silver tsunami" that the legal community is experiencing. In 2024, Texas lawyers totaled 24,109. That population represents about 21% of the 116,127 members of the State Bar of Texas as of Spring 2025.

In 2018-2019, the Bar created a Succession Planning Workgroup that was chaired by Greg Sampson out of Dallas and me, with the goal of enabling solo practitioners to easily designate a custodian who could take possession of their files and contact their clients, not for the purpose of taking over the work, but to return those files to the clients or to send them to the client's next choice of lawyer. The primary result of this workgroup was the creation of the succession planning portal on the State Bar of Texas website. Texas lawyers can use the online portal to designate a custodian attorney in less time than it will take to print a boarding pass on Southwest Airlines. The electronic designation form will allow a lawyer to designate one or more custodians. The designation prompts an email to the designee to confirm whether the designation is accepted.

In 2023, the State Bar Law Practice Management Committee created the succession planning toolkit, which is available at ***texasbarpractice.com***. It is a treasure trove of resources available for our solo practitioners who need to designate a custodian attorney and provides many resources to non-solo practitioners, as well. Only 1,500 of our more than 116,000 active Texas lawyers have designated a custodian attorney through the Bar's portal. Our solo lawyers need to prioritize their clients by designating a custodian attorney so that their clients are protected.

## RESOLVING FEE DISPUTES:

# The Vital Role of the HBA Fee Dispute Committee

**By FELICIA HARRIS HOSS**

In furtherance of the policy of the Houston Bar Association (HBA) to provide for binding arbitration of attorney-client fee disputes after efforts to resolve such matters informally have failed, the mission of the HBA Fee Dispute Committee (FDC) is to aid lawyers and clients in resolving fee-related conflicts. To that end, the FDC administers "a program and procedure for the arbitration of disputes concerning any and all fees and/or costs paid, charged, or claimed for professional services by lawyers."[1]

Established at the behest of the State Bar of Texas during the 1985–1986 Bar year, the HBA FDC has provided complimentary arbitration services for nearly four decades, ensuring a cost-efficient and fair process for resolving fee disputes. Although the need for this service remains minimal, the FDC has reliably adjudicated over 100 arbitrations since 2015, averaging more than 12 cases per year, with the number fluctuating year to year.

Consistent with standard arbitration procedures, the jurisdiction of the FDC is invoked only if the parties agree to submit their dispute to the FDC for administration. When there is such an agreement, either party—lawyer or client—can initiate the process by submitting a demand through the HBA's online portal. Once the demand is filed, along with any relevant documents, the HBA sends a copy to the respondent with a consent form to be signed confirming the parties' agreement. Thereafter, a committee co-chair appoints two lawyers and one non-lawyer to form a panel, with one lawyer designated as chair. This panel then administers the arbitration process pursuant to the FDC rules, which have been adopted by the HBA.

Like most sets of arbitration rules, the FDC rules are comprehensive, covering such things as arbitrator appointment, hearing procedures, the award and enforcement, and confidentiality. Additionally, for those volunteering time to serve on the FDC, the rules also include a provision for immunity from legal action for committee members, arbitrators, and the HBA for conduct within the scope of their official duties.[2] Awards rendered by FDC panels are subject to review upon petition to a court with jurisdiction under the Texas Arbitration Act, with provisions for attorney's fees and costs for the prevailing party.[3]

Although the jurisdiction of the FDC is narrow, it is intended to be broad enough to fully resolve fee disputes. For example, counterclaims are permissible so long as the scope is limited to challenging the disputed fee amount.[4] And if a third-party has paid or may be liable for payment of the lawyer's fee, the third party may consent to be joined by the client as a party to arbitration.[5] However, disputes involving ongoing malpractice lawsuits, grievances alleging professional misconduct, or disputes filed more than four years after the attorney-client relationship ends or the final billing are outside of the FDC's jurisdiction.[6]

The FDC arbitration process is not only very similar to the process most lawyers are accustomed to when arbitrating other disputes. It is also very efficient. For example, since 2021, the average time from initial filing to award is approximately 19 weeks, with the shortest period only 83 days.

It goes without saying that the commendable work of the committee is a byproduct of the dedicated volunteer arbitrators whose services carry out the committee's mission. Much gratitude is given to the committee members who have served over the years, and to those who serve now. At present, the committee maintains a roster of qualified lawyer and non-lawyer arbitrators, with a current tally of 30 lawyer panelists and 10 non-lawyer panelists.

Each year, the FDC offers an orientation session for panelists to learn the process and objectives of fee dispute panels, and to become familiarized with templates used in the administration of proceedings. Anyone interested in becoming a lawyer-arbitrator or wanting to recommend someone to join the non-lawyer panel can contact the HBA or this year's co-chairs, Mark Flanagan and myself, for more information. Soon, an application link will be added to the HBA Fee Dispute Committee webpage, as well.

***Felicia Harris Hoss*** *is a mediator and arbitrator with Harris Hoss PLLC, and 2024–2025 co-chair of the HBA Fee Dispute Committee. She is on the editorial board of* The Houston Lawyer.

### Endnotes

1. *See* HBA Rules and Regulations for the Fee Dispute Committee at Rule 1.01.
2. *See id.* at Rule 10.02.
3. *See id.* at Rule 8.02.
4. *See id.* at Rule 5.06.
5. *See id.* at Rule 5.10.
6. *See id.* at Rule 1.04.

## LAW PRACTICE MANAGEMENT SECTION:

# Dedicated to Assisting Attorneys in the Business Side of Law Practice

**By SHANNON ALMES**

The Law Practice Management Section is dedicated to arming attorneys with the tools needed to be successful in managing and growing their practices. The section is made up of solo practitioners, owners, and managing attorneys in small and mid-sized firms, as well as other members of management in firms and various organizations throughout the Houston area. The section serves its members by hosting monthly luncheons and other events where members can learn about and examine different aspects of the practice of law.

The focus for this Bar year has been to connect members with each other in a more meaningful way, so that we may all benefit from the different knowledge and experience we each possess. Our members specialize in all aspects of the legal profession, including probate and estate planning, personal injury, business litigation, immigration, real estate, intellectual property, and labor and employment. The CLE topics that have been presented by and to our members include: budgeting and financial planning for firms; using technology to improve your law firm's success; the specific platforms used by attorneys in the group; succession planning, presented by former Texas Bar President Laura Gibson; different legal fee structures and how to modernize fee structures; building and marketing an attorney's personal brand; self-care and mindfulness; and hiring and maintaining talent, including a look at current employment trends and laws. We have also partnered with other organizations, such as the Texas Society of CPAs and the Houston Young Lawyers Association to host events, where members share and gain knowledge from professionals in other fields.

Section members bring their many different areas of expertise to the table in presenting to the section at its monthly CLE presentations or in the lively conversations that follow many of these CLE luncheons when members can discuss the challenges they are facing in their practice or their need for input from practitioners in a different specialty. Another event our members look forward to each year is the annual holiday party because it provides members a chance to learn more about each other in a casual atmosphere outside of a one-hour lunch.

As we move into the new Bar year, the Law Practice Management Section looks forward to continuing to expand its membership to the many new and established solo and small firm practitioners in the Houston area. With the ever-changing world of practicing law, we are excited to continue to learn about the many ways we can become better lawyers and businesspeople, as well as sharing our experiences with others in the section so that we can learn from both our mistakes and our successes.

The section is grateful to the leadership of its board, many of whom have served multiple terms throughout the history of the Law Practice Management Section: Leslie Turnage, Amber Boyd, Ruby Powers, Shannon Almes, Kevin Keeling, John Moody, and John Meredith.

***Shannon Almes*** *is an employment attorney at Feldman & Feldman, PC. Shannon is currently serving as chair of the HBA Law Practice Management Section.*

# *DeVillier v. Texas*: Judicial Restraint and Exercise in Judicial Academics

**By CASSIE MCGARVEY**

*Devillier v. Texas*[1] is an example of judicial restraint. While the Supreme Court was presented an interlocutory appeal with the question of whether the Takings Clause in the Fifth Amendment provides a direct cause of action against a state, it did not decide the issue. Because plaintiffs had a remedy under Texas law, the Court declined to answer the question. As such, the question of whether the Takings Clause is self-executing and providing a cause of action remains unanswered. However, the Supreme Court was clear in this opinion that it expects the states to honor the Constitution, including the Takings Clause.

The academic decision from the Supreme Court arose from a construction project along Interstate 10 (I-10) between Houston and Beaumont. The State of Texas (through TXDOT) elevated I-10 and installed a 3-foot-tall solid concrete barrier along the median to act as a dam. The purpose of the dam was to keep I-10 clear for purposes of flood evacuations. The dam worked as intended. It kept I-10 clear of water and passable during heavy rainfalls. But it flooded the plaintiffs' land to the north.

Devillier and others filed four separate class action lawsuits against the State of Texas alleging that the median barrier and use of his property to store stormwater was a violation of the Fifth Amendment. In the state court petitions, the plaintiffs alleged an inverse-condemnation claim under Article I, Section 17 of the Texas Constitution. However, Plaintiff also alternatively alleged an additional federal inverse-condemnation claim based on the contention that the Takings Clause of the Fifth Amended itself created a federal cause of action for takings without requiring a procedural vehicle. The State believed that plaintiffs were attempting to bring a 42 U.S.C. § 1983 claim against the State, as they invoked no procedural vehicle for their federal takings claim other than an alleged general violation of the Takings Clause of the Fifth Amendment. Accordingly, the State removed the cases to federal court.

After removal, the State requested that the plaintiffs amend their petitions because it appeared that plaintiffs were attempting to bring federal claims that could not be brought directly under the U.S. Constitution and plaintiffs had otherwise failed to adequately plead a federal inverse condemnation claim. In response, plaintiffs refused to amend or move to remand because they believed the Fifth Amendment claim to be self-executing, making federal subject matter jurisdiction (and removal) proper under 28 U.S.C. § 1331. The State filed a motion to dismiss for failure to state a federal constitutional claim. The motion was denied.

Eventually, all four cases were consolidated, and the plaintiffs filed a master complaint encompassing all cases. In this amended complaint, plaintiffs stated the following claims: 1) a state inverse condemnation claim under article I, § 17 of the Texas Constitution; 2) a federal inverse condemnation claim directly under the U.S. Constitution through the Fifth Amendment's Takings Clause, 3) a procedural due process claim under the Fourteenth Amendment, and 4) a substantive due process claim under the Fifth Amendment's Takings Clause (as incorporated through the Fourteenth Amendment). The State renewed its motion to dismiss, which was denied. However, the Court noted an immediate appeal might materially advance the ultimate termination of the litigation.

On interlocutory appeal, the Fifth Circuit held that "the Fifth Amendment Takings Clause as applied to the states through the Fourteenth Amendment does not provide a right of action for takings claims against a state."[2] The Fifth Circuit later denied rehearing *en banc*.[3] In a concurring opinion, Judge Higginbotham discussed the State of Texas' commitment to the Takings Clause, in a foreshadowing of the discussion by the Supreme Court. Judge Higginbotham noted that in the absence of a federal cause of action, "[t]he pathway for enforcement in takings by the state is … through the state courts to the Supreme Court."[4] Because "[t]he Supreme Court of Texas recognizes takings claims under the federal and state constitutions," Texas fulfills its "obligations under the Takings Clause by the state."[5]

The United States Supreme Court granted certiorari to consider whether the Fifth Amendment's Taking Clause itself creates a federal cause of action for takings if the legislature has not affirmatively provided such a cause of action.[6] The Supreme Court noted that the question presented by the plaintiffs assumed the property owner had no separate cause of action.[7] But because the plaintiffs had a cause of action under Texas state law, the question presented was not applicable. Therefore, the Supreme Court vacated the appeal and remanded so that the plaintiffs' claims could proceed under Texas' state law cause of action.[8]

Following the remand, to district court, the State has filed a motion to remand the case to state court. The plaintiffs oppose the motion, contending that federal question jurisdiction existed at the time of the removal as a result of the claims under the Takings Clause and, because jurisdiction is determined at the time of removal, federal jurisdiction still exists. It remains to be seen whether a claim under the Fifth Amendment will be sufficient to raise federal question jurisdiction considering the Supreme Court's determination that the case should proceed under Texas law.

***Cassie McGarvey** is a principal attorney at McGarvey PLLC. She is board certified in both commercial and residential real estate law and is a self-proclaimed procedural nerd who enjoys the nuances of real estate cases. Outside of law, she is an avid runner, a Rotarian, and Scoutmaster for her daughters' Scouting America troop.*

## Endnotes

1. 601 U.S. 285 (2024).
2. *Devillier v. State*, 53 F.4th 904 (5th Cir. 2023) (per curiam).
3. *See Devillier v. State*, 63 F.4th 416 (5th Cir. 2023) (per curiam).
4. *Id.* at 418–19.
5. *Id.* at 417 n.2, 418.
6. *DeVillier*, 601 U.S. at 287–88.
7. *Id.*
8. *Id.*

# The Man Behind the Robe: A Personal Reflection and Review of *Scalia: Rise to Greatness, 1936–1986*

**By JAMES ROSEN**
**Published by Regnery Publishing**
**Reviewed by RINKU RAY**

My first impression of Justice Antonin Scalia was not from a law review or a court opinion, but from a chance encounter in May 1990. I was a bleary-eyed underclassman, sitting down to lunch with classmates after finishing my last exam of the semester. Despite the academic year winding down, the campus dining hall was unusually lively—families of graduating seniors had arrived early for the next day's commencement, mingling with students over lunch.

At the center of the room sat a strikingly large family, dressed just a bit more formally than most. They didn't draw attention with flash, but with presence—a natural charisma, a sense of warmth and polish. One man in particular stood out. Stout, with a receding head of dark hair and a deep, resonant voice, he held the table in rapt attention as he told a story, gesturing animatedly. Laughter erupted around him. Other parents noticed. Students glanced over. I tried to place him. That is when an upperclassman leaned over and said, "That's Supreme Court Justice Scalia. He's here for his daughter's graduation."

Years later, I encountered Justice Scalia again—this time through reading his opinions as a law student. I was struck by the contrast between the jurist whose voice was rooted in originalism and textualism, and the convivial father I had briefly observed years earlier. That dissonance—between the man and the robe—sparked a deeper curiosity in me: Who was Justice Scalia, really?

That question led me to James Rosen's biography, *Scalia: Rise to Greatness, 1936–1986.* James Rosen, a seasoned journalist and historian, weaves together content from personal interviews, previously unpublished writings, and archival research into a biography that reads like a novel, full of arcs, dialogue, and settings with vivid human detail. It is a portrait not just of a legal philosophy, but of a life—one shaped by faith, family, ambition, and a relentless pursuit of intellectual clarity. Over the course of seventeen (17) chapters, Rosen develops a portrait of "the kid from Queens, the Immigrant's son with the Ivy League credentials and a winning way with words" whom family and friends called "Nino." Rosen portrays Scalia not merely as a jurist, but as a well-liked, affable man with a capacity for hard work and a love of debating legal ideas.

The book opens, not with Scalia's birth in 1936, but with his unanimous 98-0 Senate confirmation as the youngest, and first Italian-American in history to be named Supreme Court Justice in 1986. The rest of the book, rewinding all the way back to Scalia's family roots in Italy, serves as a backstory, offering an in-depth exploration of the influences, experiences, and principles that shaped his first 50 years of life and his legal philosophy. Rosen traces Scalia's unwavering self-belief, grounded in hard work and a drive for excellence, in academics, debate, drama, music, and languages, back to his early family life. As the only child and the center of attention in a large, close-knit, education-focused immigrant family, Scalia was deeply shaped by the values and expectations that surrounded him from a young age. He chronicles Scalia's academic achievements—graduating as valedictorian from both Xavier High School, a Jesuit Catholic military academy and Georgetown University, as well as graduating magna cum laude from Harvard Law, where he met his wife, Maureen.

Rosen follows Scalia's "rise to greatness" through a chronological account of his diverse and distinguished career, beginning with a brief but successful stint in private practice at a prestigious law firm. He illustrates how Scalia's views on constitutional interpretation began to crystallize during his years as a law professor at the University of Virginia. In his public roles under the Nixon and Ford administrations, Scalia further honed his textualist, originalist philosophy, insisting that even unpopular constitutional principles (like executive privilege or separation of powers) must be upheld as written. On his return to academia at the University of Chicago, Scalia played a key role in shaping and legitimizing the core philosophies of the Federalist Society—originalism and textualism. Scalia's career path culminates in his appointment to the U.S. Court of Appeals for the D.C. Circuit, paving the way for his eventual rise to the Supreme Court.

Rosen also gives space to the deep love Scalia had for his wife, Maureen, his nine children, his colleagues, and his students. Rosen references "The RBG and Nino papers," unpublished correspondence culled from 223 boxes of Ginsburg's files in the Library of Congress to address the mutual admiration, warmth, and affectionate friendship that blossomed between Antonin Scalia and Ruth Bader Ginsburg during their time on the D.C. Circuit. Rosen also weaves in personal and professional challenges, offering a nuanced and humanizing portrait of Scalia that goes beyond his public persona, giving readers a fuller understanding of the man behind the robe.

Reading *Scalia: Rise to Greatness* provided me with a richer perspective on the man I had glimpsed decades ago in the dining hall. It reinforced the complexity of Justice Scalia—both as a legal titan and as a devoted family man. For those interested in understanding the roots of Scalia's jurisprudence, as well as the personal experiences that shaped him, Rosen's biography is an invaluable resource.

***Rinku Ray*** *is the founder and managing attorney of Ray & Fahys, PLLC, a firm focusing on business immigration law, and is on the editorial board of* The Houston Lawyer.

# Join the HBA 100 Club!

**The Houston Bar Association 100 Club is a special category of membership that indicates a commitment to the advancement of the legal profession and the betterment of the community. The following law firms, government agencies, law schools and corporate legal departments with five or more attorneys have become members of the 100 Club by enrolling 100 percent of their attorneys as members of the HBA.**

### Firms of 5-24 Attorneys

Abraham, Watkins, Nichols, Agosto, Aziz & Stogner
Ajamie LLP
Alvarez Stauffer Bremer PLLC
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC
Buck Keenan LLP
Christian Levine Law Group, LLC
Coats | Rose
Crady, Jewett, McCulley & Houren, LLP
De Lange Hudspeth McConnell & Tibbets LLP
Dentons US LLP
Dobrowski Stafford LLP
Doyle Restrepo Harvin & Robbins LLP
Ewing & Jones, PLLC
Fisher & Phillips LLP
Fizer Beck Webster Bentley & Scroggins
Fogler, Brar, O'Neil & Gray LLP
Frank, Elmore, Lievens, Slaughter & Turet, L.L.P.
Funderburk Funderburk Courtois, LLP
Germer PLLC
Gordon Rees Scully & Mansukhani, LLP
Hagans
Henke, Williams & Boll, LLP
Hirsch & Westheimer, P.C.
Holm | Bambace LLP
Horne Rota Moos LLP
Hughes, Watters & Askanase, L.L.P.
Husch Blackwell LLP
Jackson Lewis P.C.
Jenkins & Kamin, LLP
Johnson DeLuca Kurisky & Gould, P.C.
Jordan, Lynch & Cancienne
Kean Miller
Kilpatrick Townsend & Stockton LLP
Law Feehan Adams LLP
Linebarger Goggan Blair & Sampson, LLP
Liskow
McGinnis Lochridge
McGuireWoods LLP
McKool Smith
MehaffyWeber PC
Morris Lendais Hollrah & Snowden
Murrah & Killough, PLLC
Nathan Sommers Jacobs
Ogletree Deakins Nash Smoak & Stewart, P.C.
Paranjpe Mahadass Ruemke LLP
Peckar & Abramson, P.C.
Phelps Dunbar LLP
Pillsbury Winthrop Shaw Pittman LLP
Ramey, Chandler, Quinn & Zito, P.C.
Rapp & Krock PC
Reynolds Frizzell LLP
Roach & Newton, L.L.P.
Ross Banks May Cron & Cavin PC
Royston, Rayzor, Vickery & Williams, L.L.P.
Rusty Hardin & Associates, LLP
Schirrmeister Diaz-Arrastia Brem LLP
Schwartz, Page & Harding, L.L.P.
Scott, Clawater & Houston, L.L.P.
Shannon Martin Finkelstein Alvarado & Dunne, P.C.
Shearman & Sterling
Shellist | Lazarz | Slobin LLP
Shipley Snell Montgomery LLP
Smith Murdaugh Little & Bonham LLP
Sorrels Law
Spencer Fane
Sponsel Miller Greenberg PLLC
Stuart PC
Taunton Snyder & Parish
Thompson & Horton LLP
Tindall England PC
Tracey & Fox Law Firm
Ware, Jackson, Lee, O'Neill, Smith & Barrow, LLP
West Mermis
Weycer, Kaplan, Pulaski & Zuber, PC
Williams Hart & Boundas, LLP
Wright Abshire, Attorneys, PC
Wright Close & Barger, LLP
Ytterberg Deery Knull LLP
Zukowski, Bresenhan & Piazza L.L.P.

### Firms of 25-49 Attorneys

Adams and Reese LLP
Andrews Myers, P.C.
Beck Redden LLP
BoyarMiller
Bradley Arant Boult Cummings LLP
Bush & Ramirez, PLLC
Cokinos | Young
Gibbs & Bruns LLP
Hogan Lovells US LLP
Kane Russell Coleman & Logan PC
Littler Mendelson P.C.
Martin, Disiere, Jefferson & Wisdom LLP
McDowell & Hetherington LLP
Wilson Cribbs & Goren PC
Yetter Coleman LLP

### Firms of 50-99 Attorneys

AZA Law
BakerHostetler LLP
Brown Sims, P.C.
Chamberlain Hrdlicka
Greenberg Traurig, LLP
Haynes and Boone, LLP
Jackson Walker LLP
Morgan, Lewis & Bockius LLP
Susman Godfrey L.L.P.
Winstead PC

### Firms of 100+ Attorneys

Baker Botts L.L.P.
Bracewell LLP
Hunton Andrews Kurth LLP
Norton Rose Fulbright
Porter Hedges LLP
Troutman Pepper Locke LLP
Vinson & Elkins LLP

### Corporate Legal Departments

CenterPoint Energy, Inc.
EOG Resources, Inc.
MAXXAM, Inc.
Plains All American Pipeline, L.P.
Quantlab Financial, LLC
Rice University
S & B Engineers and Constructors, Ltd.

### Law School Faculty

South Texas College of Law Houston
Thurgood Marshall School of Law
University of Houston Law Center

### Government Agencies

Harris County Attorney's Office
Harris County District Attorney's Office
Harris County Domestic Relations Office
Lone Star Legal Aid
Metropolitan Transit Authority of Harris County, Texas
Port of Houston Authority of Harris County, Texas
1st Court of Appeals
14th Court of Appeals

SORRELS LAW


# New Houston Office
# New Collaborations

Sorrels Law announces our move to a spacious new Houston office at 230 Westcott. The new facility features four well-appointed conference rooms, available to fellow legal professionals at no cost. We collaborate with lawyers across Texas and, with free parking and free conference rooms, we want to collaborate with you too.

Specializing in catastrophic personal injury, wrongful death, product liability, medical malpractice, and business dispute litigation, our experienced team of lawyers is ready to joint venture on matters with your firm. We also welcome referrals and offer competitive referral fees.

Connect with Sorrels Law — let's work together to achieve justice for our clients.

Best Lawyers LAWYER OF THE YEAR RANDALL O. SORRELS 2023
Best Lawyers LAWYER OF THE YEAR RANDALL O. SORRELS 2022
Best Lawyers LAWYER OF THE YEAR RANDALL O. SORRELS 2018
BEST LAW FIRMS 2024
TEXAS TOP 100 HOUSTON TOP 100 Super Lawyers Randall O. Sorrels
Best Lawyers LAWYER OF THE YEAR RANDALL O. SORRELS 2016
Best Lawyers LAWYER OF THE YEAR RANDALL O. SORRELS 2013

**Houston Office - Main:** 230 Westcott St., Houston, TX 77007 | (713) 496-1100 | www.SorrelsLaw.com
**Austin Office:** 2901 Bee Cave Road, Suite L, Austin, TX 78746 **Dallas Office:** 3010 Lyndon B Johnson Fwy., Suite 1450, Dallas, TX 75234