COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

Volume 3: Winter 2015

TABLE OF CONTENTS

Letter from the Chair – ILTA Announcement

By Joseph Jacobson

FREE resources and discounts increasing your efficiency and helping maintain ethical compliance are just clicks away

You now have FREE membership in the International Legal Technology Association (ILTA).

Meet your fellow members

Susman Godfrey L.L.P., U.S. Dept. of Justice, U.S. Securities & Exchange Commission, Baker Botts L.L.P., Dell, Inc., the Law Society of Upper Canada, Kelly Hart & Hallman LLP, 3M Company, Kroger Co., Texas Instruments Inc., Baylor Law School, and the Walt Disney Company are all ILTA members.

Now you've joined them, without charge. What's in it for you?

What ILTA offers you and other members

With access to publications, peer groups, online discussion forums, Webinars and more, ILTA members stay up-to-date on the latest legal technology and participate in a free-flowing exchange of knowledge and ideas.

Start taking advantage of all that ILTA has to offer! You must register on ILTA's web site and then you can see not only the public information, but the member's only material.

Please read the following instructions to guide you through the quick and easy registration process. ****To register with ILTA you must use an email address with the Computer & Technology Section's domain, @sbot.org.**** (An email address belonging to the C&T Section's domain is necessary for free access to ILTA, but this email is NOT to be used for other purposes.) See below for details.

Create a User Account with ILTA

1. Open ILTA's website: www.ILTAnet.org.

2. Click the login button located near the top-right corner of the page.

3. On the login page, select the option to register for a new account.

I would like to register for a new account. Click here to register.

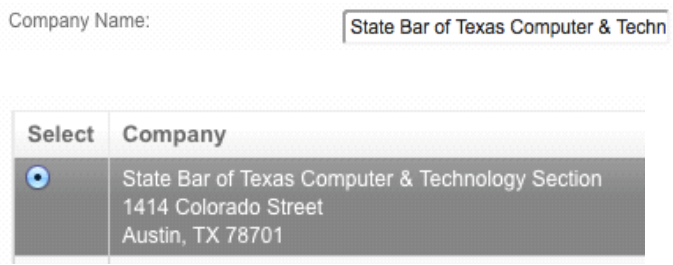
4. The “Tell us about yourself” page opens with a space to enter your email address. ****IMPORTANT – You must enter an email address with the C&T Section’s domain, @sbot.org.**** Please use the format firstname.lastname@sbot.org. Example: C&T Section Member, Jane Smith, will enter the email address: jane.smith@sbot.org.

Because the email addresses must be unique, a few users might need to add their middle name or initial. If your email address is not validated on the first attempt, please enter firstname.middlename.lastname.@sbot.org. And finally, if that email is not validated, please enter firstname.middleinitial.lastname@sbot.org.

NOTE: Creating this email address was necessary to provide C&T Section members free access to ILTA. It should be used only for ILTA membership. This is NOT a permanent email address.

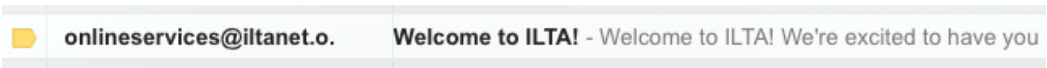
5. After entering your email address, click the **Continue** button.

6. Continue following on-screen instructions and populating required fields. You will notice that some of the fields auto-populate with the Computer & Technology Section information. Please do not change this information.



7. After populating all required information, enter and confirm your password and click the **Next** button.

8. CONGRATULATIONS! Your account page should appear displaying your contact information and your Company/Firm Name as the State Bar of Texas Computer & Technology Section. Also, most of you will receive an email from ILTA in your inbox, confirming your account has been created.



If you received this email, the C&T Council has already arranged for ILTA-generated emails to be forwarded to the email address you provided to the State Bar of Texas.

If you did NOT receive a "Welcome to ILTA" email and would like to receive ILTA-generated emails in the future, please notify the C&T Council and we will ensure that ILTA emails are forwarded to your preferred email address. **Warning: Your email address at sbot.org is not accessible by you directly.**

If you are no longer a member of the Section, then you will lose all rights to your @sbot.org email address.

The C&T Section Council is excited to offer you this valuable opportunity to join ILTA…for FREE!

If you have questions or problems registering, please contact website@iltanet.org. If there is a problem that ILTA cannot resolve, have ILTA contact us.

Best regards,

Joseph Jacobson, Chair of the Computer & Technology Section

P.S. Register now at ILTAnet.org using your new C&T Section email address to receive FREE resources, access to Webinars, and discounts to CLE.

Letter from the Editor

By Michael Curran

Welcome to our third edition of Circuits, a newsletter for the State Bar of Texas Computer & Technology Section. As always, this newsletter would not be possible without the support of our contributing authors. Security breaches are all around us these days, and we are grateful to have articles by two authorities on this hot topic. Many thanks to Elizabeth Rogers and Shawn Tuma for their practical information regarding how to help your clients prepare for and respond to data breaches. In addition, we have our first ever co-authored article in this issue. Jason Rodriguez and Thomas Allen both volunteered to write about Bitcoin. After a few short emails, Jason and Thomas decided to join forces to provide Texas attorneys with an introduction to Bitcoin – a new form of crypto-currency that you may wish to consider. Much appreciated gentlemen. Finally, I would like to thank the co-editors Craig Ball and Antony P. Ng and section member Sanjeev Kumar for reviewing this edition's articles. I appreciate all your hard work.

As mentioned by Section Chair Joseph Jacobson, members of the Computer & Technology Section are now able to join the International Legal Technology Association ("ILTA") at no cost. The normal starting minimum ITLA fee is $375 for a small law firm. As a section member, you are getting all the benefits of ITLA membership without paying the membership fee. What a bargain! I have participated in ILTA events and reviewed their publications in the past. I hope that you agree that this is a first-class organization with many great resources, and please enjoy this new perk.

In other news, the Computer & Technology Section is planning a legal technology CLE course for a smaller legal market in Texas. Attorneys in Houston, Dallas and Austin have numerous opportunities to attend a CLE that focuses on legal technology. In the coming months, the Computer & Technology Section is going to offer members in one of our smaller legal markets the opportunity to attend an in-person CLE focused on legal technology issues. For section members who are not able to attend the small market CLE, the Computer & Technology Section will once again be co-sponsoring the Adaptive Lawyer track to offer educational information regarding legal technology during the State Bar of Texas Annual Meeting.

If you would like to become an author of an article for an upcoming issue of *Circuits*, please contact Michael Curran at michaelcurranpc@gmail.com or 512-800-9017.

Practical Cyber Law: Yes, Even Your Clients May Face Cyber Risk Issues

By Shawn Tuma

Lawyers in different practice areas, especially those that involve business, can expect to start seeing cyber risk issues arising with their clients more frequently. While that statement may come as quite a shock to many, before going further, I recognize what you may be thinking: "but my clients are just general businesses, they are not in the high-tech business, so how does this apply to me?"

Because of the prevalence of cyber risk in today's business environment, cybersecurity and data privacy issues arise in a wide variety of business relationships. Unless your clients do not (1) use a computer, (2) receive, store, or transmit electronic data, or (3) connect to the Internet — and do not do business with any company that does — your client's business could be impacted by cybersecurity and data privacy issues.

If any of your clients found themselves in such a situation, oftentimes you will be their first line of defense. By having a basic understanding of these issues, you will be able to give them much better guidance, even if that guidance is simply referring them to someone who has expertise in handling the relevant issues.

Two Real-Life Examples of How Lawyers Who Represent Business Clients Can Face Cyber Issues

The recent Target data breach provides an excellent illustration of this point. Did you know that the hackers that compromised Target's point of sale system and stole its payment card data did not "hack" into Target's system directly? Instead of attacking Target head-on where Target's defenses were strongest, they followed the ancient lessons of warfare and used an indirect method of attack to strike Target where its defenses were weaker.

The hackers did this by using a common email "click here" scheme, that when opened by an unsuspecting employee of Fazio Mechanical Services, deposited malware on Fazio's network. Fazio was one of many third-party vendors that provided HVAC services to Target. Once the hackers' malware was on Fazio's network, they used it to "sniff" the network and find the login credentials Fazio used to access Target's portal that vendors used for submitting electronic billing, contracts, and project management data. This provided the hackers with their entry

point into Target's network. Once they were inside the perimeter of Target's network, they were in a much better position to unleash their attack on Target.[1]

Cyber risk knows no boundaries and can impact every kind of business. Target is not a technology company. Target is not involved in a particularly technology-heavy industry. Target is a retailer that was attacked because it has data that is valuable. Target uses technology in its business operations and, while that technology is a valuable asset, it also proved to be a vulnerability. Fazio is an HVAC company that is likewise not in a particularly technology-heavy industry. Fazio used technology in its business operations and, because its (likely largest) customer required it to integrate its technology, Fazio was attacked because it provided an entry point into its customer's computer network.

While your clients may not be an industry giant like Target, they could easily be an entry point to one such as a Fazio. As of the time of this writing, there is no report of Target having taken formal legal action against Fazio because of this breach but that does not mean that Target cannot or will not. Indeed, for a smaller company like Fazio, simply losing the business of a customer like Target could be enough to put the company out of business. These are serious matters. The Target case, however, is not the only example of how third parties can be used to execute such attacks and the risks that come with them.

Last year, a group of hackers were trying to hack into the network of a large oil company but were unable to breach its network with head-on attacks. Considering the indirect method of attack, after learning that a Chinese restaurant located near the company's office was popular with the company's employees, they infected the restaurant's online menu with malware. When the employees using the company's computers visited the menu, they inadvertently downloaded the malware which gave the attackers the entry point they needed into the company's computer network.[2]

Neither the oil company nor the restaurant was a technology company. But, one had valuable data and one was a vehicle that provided a means for gaining access to the other's computer

---

[1] 11 Steps Attackers Took to Crack Target, CIO Online, http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html (last visited Jan. 25, 2015).

[2] Hackers Lurking in Vents and Soda Machines, The New York Times, http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html?_r=0 (Apr. 7, 2014).

network. Do you have clients that have valuable data? Do you have clients that have websites or other forms of digital connections to companies that may have valuable data?

Hackers are very creative. As more companies work to strengthen their own defenses, this kind of indirect method for attacking their primary targets is becoming more common. Not only do businesses now face cyber-attacks directed at them, but now they may also face cyber-attacks because of their relationships with other businesses. The pool of potential cyber-attack victims is expanding exponentially.

Practical Lawyers Should Be Able to Recognize the Cyber Issues as Their Clients' First Line of Defense

As the variety of businesses involved in cyber-attacks increases, the lawyers who represent them will start seeing more of these issues arise. As their clients' first line of defense in many cases, lawyers who have enough familiarity with cybersecurity and data privacy issues to alert their clients from the beginning will be doing them a great service. The rules and regulations of various industry groups and governmental authorities are evolving rapidly and their time for compliance can be very short. Businesses that find themselves in these situations must respond quickly. If they do not, then the consequences can be much worse.

While you may not wish to become an expert on cybersecurity and data privacy issues, it is helpful for you to be able to identify the issues well enough to recognize that someone needs to address them. In the right situation, that advice can be invaluable to your clients. That is practical lawyering in the 21st Century.

About the Author

Shawn Tuma (@shawnetuma) is a cybersecurity lawyer business leaders trust to help solve problems with cutting-edge issues involving cyber risk and compliance, computer fraud, data breach and privacy, and intellectual property law. He is a partner at Scheef & Stone, LLP, a full service commercial law firm in Texas that represents businesses of all sizes across the United States.

The Corner Privacy Counselor: How to Prepare for Breach Readiness and Breach Response

By Elizabeth Rogers

Thirteen years after California passed the first ever breach notification law in 2002, there are now only 3 states (Alabama, New Mexico and South Dakota) that do not have one. And, while most all of the United States have embraced the need for consumer identity theft remedies and notification legislation, there are almost as many differences in each state's law as there are states. It is within this context that the federal government has become more proactive in addressing the public outcry that immediately followed the substantially invasive and massive hack of Sony Entertainment, by proposing a national standard for definitions of sensitive personally identifiable information and a deadline for breach notification.

Until Congress agrees on uniform responsibilities and liabilities; however, our multistate clients must traverse the patchwork of laws in 47 states and the District of Columbia, in addition to the regulations of multiple federal agencies who have assumed oversight roles for privacy and security practices. Among this state of uncertain standards, how do we manage our role as trusted advisors for our clients?

For now, we can take comfort in recommending some practical tactics that are designed to mitigate the risks of a breach occurrence while contemporaneously laying the foundation for a litigation defense strategy in the event that one occurs. In either case, these steps will go a long way in reducing the cost of a breach and/or the potential cost of a settlement with regulators and/or class action litigants. So, without regard to whether any law requires these following steps, we provide a valuable legal service by advising clients to observe the proper standard of care that applies to their data and the employees and other authorized third parties that handle it.

Develop a Robust Privacy and Information Security and Awareness Training Program

When it comes to news about data breaches, the hackers and the criminals are the headline grabbers but, statistics show that most data breaches are caused by insider threats – or employee mistakes and system glitches caused by employees taking shortcuts. According to Michael Bruemmer, vice president of Consumer Protection at the credit reporting and financial services firm Experian, of 3,100 incidents that Experian Data Breach Resolution serviced in 2014, "81% had a root cause in employee negligence. The most common issue was the loss of administrative credentials – user name and password – but also included lost media, firewall

left open, lost laptop etc.," he said. While user error and employee laziness are the most vulnerable link in a company's privacy perimeter, it is also the most under-reported and therefore, least emphasized area of a company's time and resources.

Our role as a practical counselor involves helping clients to hand-select the training that is best suited for them according to relevant federal and state laws that control their particular industry sector. Beyond what laws control the industry sector, however, we should also encourage our clients to focus on mitigating the risks that arise from every-day threats, such as how to detect and avoid a phishing campaign and rules for password strength and complexity.

If the client deploys threat monitoring technologies (e.g., data loss prevention tools and/or others), be sure to include awareness of the lack of privacy expectations in the training as well as critical user friendly information about how the technology operates and what it does. Many companies are also increasingly in need of guidance about laws and best practices that apply to mobile data on smartphones and other portable devices. For example, in a global company, this data may "cross borders" if hosted by a cloud provider in a foreign jurisdiction. Therefore, keep in mind that the key drivers behind any training program that is developed or purchased should be awareness of what data the client has, where and when it is processed and by whom.

Develop a Written Information Security Response Plan ("ISRP")

One of the best favors that a client can do for themselves is to have a prepared Information Security Response Plan (ISRP) for breach response and cyber crisis communications that is mapped to the strictest laws controlling their operations. For example, if company has a California presence, then it would be prudent for the plan's operative breach notification deadline to be mapped to that of California. An obvious benefit of mandating responsive behavior according to the strictest laws that control the company is the ability to satisfy standards that are less strict in other jurisdictions of operation. Another positive result for mandating the strictest standards for post breach response is the ability to demonstrate to federal and state regulators that the company takes its consumers' welfare seriously.

The process of drafting or updating an ISRP is also one of the most ideal ways of bringing all key stakeholders to the same table for a holistic approach to information privacy and security. In other words, to the extent applicable, encourage your clients to invite a Board member, members from the offices of risk management, compliance, general counsel, communications, and human resources in addition to the traditional members of the response team from information security, privacy and information technology. This assembly of thought leaders will

not only provide a valuable perspective from their own respective trenches but also will have an understanding of and preparation for key first steps that should be taken in the immediate aftermath of a breach. Again, this effort shows a post-breach jury or federal and/or state regulator that your client is aware of its responsibilities to protect consumer data and to provide them with the notice that the strictest law requires if it is compromised.

Of course, every final draft of an ISRP should be immediately followed by at least a day-long session of table top exercises. Unfortunately, most any newspaper from any city on any day of the week will provide the table top organizer with the ideal scenario. Consider having a two-day session and wait to let the stakeholders know that it's an exercise until the second day. Consider extra emphasis on privilege issues arising from communications between computer forensics experts and, if applicable, whether separate counsel should be hired for the Board to consider disciplinary issues and potential shareholder litigation. Make sure that the risk management or compliances offices know their roles about when to trigger notice to the cyber security insurance, as well.

Help Your Clients Understand the Value of Healthy Relationships with Breach Response Vendors and State and Federal Regulators before a Breach Occurs

One of the key tools in any breach response kit is a strong relationship with breach response vendors and staff members of federal regulators and the state's Attorney General's consumer protection and/or privacy divisions. While it's easy to paint any breach in black and white (in terms of the consumer victim up against the bad company with a negligent security system), most regulators know that the company is often a victim too. We all now realize there will never be a silver bullet for breach prevention and so regulators, too, are aware that hacks will happen no matter how mature a company's breach mitigation strategy happens to be.

With respect to regulators and law enforcement, reach out to the relevant Attorney Generals, Secret Service, FBI, and any other relevant regulator to introduce your client's business and discuss data security issues as soon as possible. It shows that your organization is serious about data protection and privacy and might earn your regulators' trust and respect. By meeting those who protect consumers before a data compromise occurs, your clients will have established a prior personal relationship that may aid them when it comes time to report a data breach, and the regulators may be more inclined to offer advice, listen to the client's side of the story, and give the client the benefit of the doubt about risk mitigation steps that they have taken.

Also, your client will not want to be making difficult decisions about third-party vendors in the middle of a breach response. There are several categories of third-party vendors who perform critical functions and are needed during a data breach. The most relevant to investigate provide the following services: computer forensics, public relations, notification activities, consumer remedies (credit monitoring and identity theft), call centers, and legal services. So, if at all possible, refer your clients to several options in each category and set up introductions so they will know which ones give them the greatest comfort level before the chaos begins.

If you have been brought in after the fact of breach declaration, be sure to keep your client away from the panic button and allow you to calmly guide them through each step. While many companies are in denial and do not want to notify anyone, others are too quick to publish notifications that have inaccuracies or misstatements. So, finding that goldilocks 'just right' timing is something that usually can be finessed only with the advice of a counselor who has dealt with regulators before. Point out the requirement for defining and documenting each conversation and point out how risky it is to talk with regulators without advance input from or representation by you. They will need your reminders that a key to successful resolution of regulatory investigations, in the aftermath of a breach, is communication that is timely, transparent and responsive. Encourage your client to involve you throughout the entire process so that all notes and reports are privileged, no matter how minor the call.

Conclusion

Because this is an area of law practice that was born only in this 21st century, we all have much to learn about best practices before and after a security breach. The more that we can collaborate with stakeholders at all levels of all industries, the more practical lessons we will learn and the more prepared we will be, and our clients will be in turn.

About the Author

Elizabeth C. Rogers, a shareholder in Greenberg Traurig's Austin office, focuses her practice on data privacy and cyber security matters, including those related to privacy program development (governance and policy), counseling about global privacy regulations, negotiating privacy and information security controls in third-party vendor contracts, cyber insurance and breach response. Prior to joining the firm, Elizabeth served as the first Chief Privacy Officer in Texas state government and developed a model privacy program that she shared with other data privacy professionals in agencies throughout Texas and other states.

Why Law Firms Should Accept Bitcoin

By Jason Rodriguez and Thomas Allen

In the last 12 months, Bitcoin has received quite a bit of buzz in the media. Despite its price volatility, Bitcoin's trading volume per day has increased dramatically and Venture Capitalists from all over the world are investing millions of dollars in Bitcoin development companies. In both positive and infamous news stories, Bitcoin has graced the covers of the New York Times, USA Today, Time, Bloomberg Businessweek and countless others, often in connection with illicit transactions. While economists have called Bitcoin everything from "evil" to "ingenious and elegant," one thing is for sure: Bitcoin is here to stay. So law firms should consider the benefits and risks of accepting Bitcoin and other crypto-currencies as a form of payment from their clients.

What is Bitcoin?

Bitcoin is one of the several crypto-currencies that are exchanged electronically and are generally outside of sovereign control. Indeed, Bitcoin is not a "coin" at all in the traditional sense. Rather, a bitcoin is essentially a complex mathematical code that is recorded on a public ledger as one bitcoin. That bitcoin has two security keys -- a public key and a private key -- which permit the bitcoin to be owned by (and transferred to) a person.

The public key allows the bitcoin to be utilized by the bitcoin exchanges. The private key is used by the bitcoin holder to transfer the bitcoin value to the recipient. So a bitcoin "wallet" does not hold any coins (or currency), but rather the bitcoin private keys. When someone spends bitcoins from their wallet, they are using the private key to tell the online public ledger to reflect a transfer of bitcoin to a new owner. That new owner gets a new private key and the bitcoin transaction is complete.

While the mathematics and cryptography are significantly more complicated than that, from a consumer standpoint, this is essentially how a transaction works.

Unlike sovereign issued currency, Bitcoin is not issued or backed by any government and has very little government regulation. Specifically,

- There is no Federal Reserve or similar body for Bitcoin.
- There is no government that produces bitcoins.
- Regulations and enforcement (or the lack thereof) vary significantly globally.

- All bitcoins are produced by "mining," which is basically utilizing a very complex mathematical proof to create the one-of-a-kind number that is the bitcoin.

The amount of computing power necessary to mine bitcoins is significant because of the complexity of the process. Thus, Bitcoin exchanges commit resources to this process and will offer exchange services, payment services, wallets, and other ancillary quasi-banking services to consumer account holders.

However, after you get past the complex math of a bitcoin, it is essentially just currency that can be transferred (spent) electronically with some level of privacy.

Benefits to Accepting Bitcoin

The biggest benefit to law firms considering accepting Bitcoin is the lower transaction fees. Bitcoins can be exchanged between two people, over any distance, almost immediately, with negligible transaction fees. This can be especially beneficial for international clients where exchange fees and international banking fees for local currencies can add up to around 5% onto all transactions. Additionally, credit card companies, whether for international or local transactions, typically charge about 3% per transaction. Bitcoin fees operate differently and are a little strange to people who have never used Bitcoin. All fees are voluntary but all transactions must be confirmed by the Bitcoin network, which will prioritize the confirmations based on the fees included by the user. Regardless, the transaction fee for large transfers is currently around 40 cents.

After talking with three attorneys whose firms have recently started accepting Bitcoin as a payment option, we found other benefits to accepting Bitcoin that may not be as obvious and quantifiable as the lower transaction fees: free marketing and advertising received as a result of accepting Bitcoin. Due to the novelty of the new technology and the headlines in major media outlets about Bitcoin, the three firms that started accepting Bitcoin were all featured in their local news for accepting Bitcoin. These firms put a priority on staying on the cutting edge of technology and innovation, and accepting Bitcoin is an easy way for a firm to be an "early adopter" of technology and remain competitive with larger and less nimble firms. The free advertising was also directly linked to acquiring new clients in at least two of the three firms.

Legality and Other Risks

One of the first questions when considering whether law firms should accept Bitcoin as a payment method is whether or not the transaction of accepting Bitcoin is even legal. The short answer to this question is: yes. Accept Bitcoin in exchange for legal services is just as legal as

accepting gold or flowers or anything else. The Model Rules allow it, as long as the fee for legal services is "reasonable".

The next issue law firms want to address is risk. Bitcoin has an exchange rate with the US Dollar that can be found on many different Bitcoin/Dollar exchanges online. If you look at the history of the exchange rate you will immediately notice that the price of Bitcoins is highly volatile. It is not uncommon for the price to swing 15-20% in a single day. This volatility can be attributed to many things, but there are ways to protect yourself and remove this risk completely. In addition to the volatility, the recent collapse of several Bitcoin exchanges has shed light on the added risk of relying on the Bitcoin exchanges themselves.

Another risk that may cause a law firm to be hesitant in accepting Bitcoin is Bitcoin's reputation as a medium of exchange for illicit activities. While Bitcoin has been used for its pseudo-anonymous properties to purchase illegal drugs, the vast majority of Bitcoin transactions are for legal purchases. In fact, it is estimated that drug purchases account for 1% of world GDP when measured in national currencies, whereas the total purchases of drugs online as a percentage of total bitcoin transactions was only 0.5%. However, despite these numbers, the reputation of Bitcoin is still based on the perception. Fortunately, the perception is improving as usage grows and large companies such as Overstock.com, Dell, and Microsoft, continue to accept Bitcoin.

Where to Begin

Let's assume that as a law firm considering accepting Bitcoin, you are experts in law but not exactly experts in Bitcoin. Maybe you are interested in accepting Bitcoin to lower costs or draw in more clients, but are not interested in holding the bitcoins yourself. Well, you are in luck. There are several companies in the United States (Coinbase, BitPay, et al.) that specialize in setting up businesses to accept Bitcoin and most offer a service that allows you to immediately convert all (or a percentage of your) transactions to US Dollars. These companies assume all the risk surrounding Bitcoin's current volatility. So if you receive a payment for law services rendered in Bitcoin the only thing you will see is US Dollars hitting your bank account. They typically use the average exchange rate on several exchanges and guarantee that rate at the time you receive the Bitcoins. It's similar to what credit card companies do when they set up a business to accept credit cards, only these exchanges charge much lower fees. So your firm gets the benefits of lower transaction costs and a wider client base without dealing with the volatility or the hassle of dealing with exchanges directly.

Once you have decided that you want to accept Bitcoin, the first thing you should do is learn as much as you can about it. Bitcoin does not have a central authority that issues or controls the value of Bitcoins or a company to contact for chargebacks; therefore, it is very much a caveat emptor environment. The best way to start accepting Bitcoin is to contact one of the many companies that help businesses jumpstart this process. These companies can both advise you and alleviate some of the associated risks.

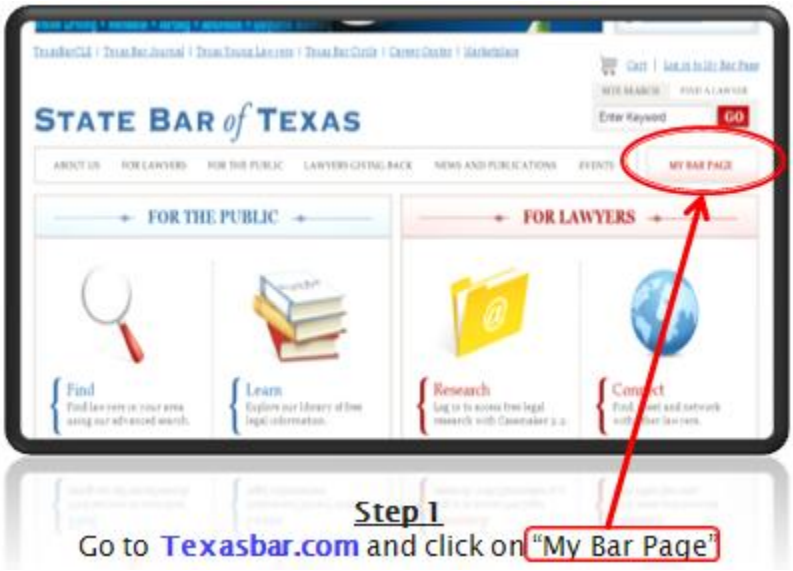
About the Authors

Jason Rodriguez is an associate at the firm Higier Allen & Lautin, PC in Addison, Texas. Jason's practice focuses on corporate bankruptcy matters and commercial civil litigation. Jason can be reached by phone at 972-716-1888 or by email at jrodriguez@higierallen.com.

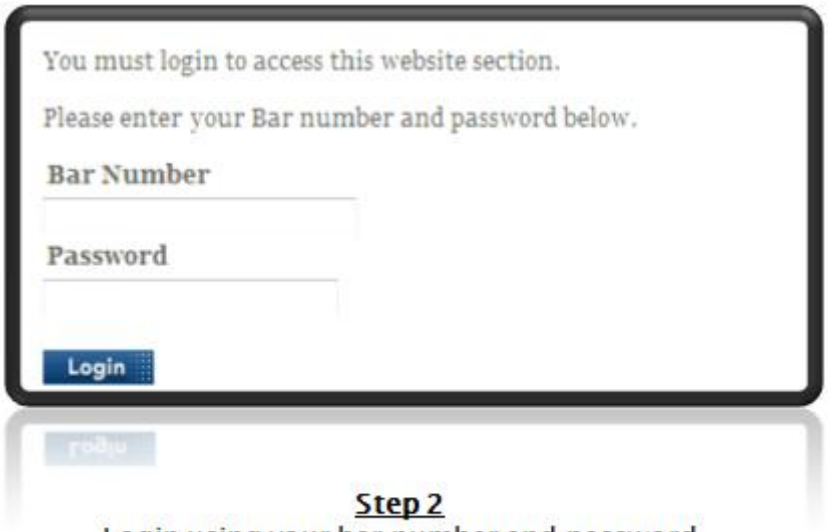
Thomas Allen is the Founder and CEO of AgileLaw, an Austin-based startup that provides paperless deposition software to litigators. Much of the content for this article was taken from a company blog post written by Patrick McElroy, a former AgileLaw employee, who is actively involved in the online and local Bitcoin communities. Thomas can be reached at thomas@agilelaw.com.

How to Join the State Bar of Texas Computer & Technology Section

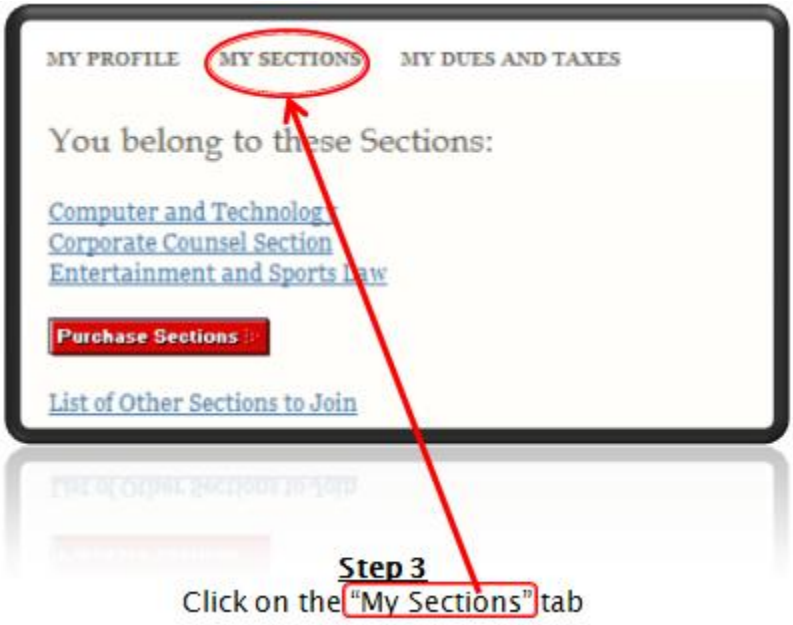
Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



Step 1
Go to Texasbar.com and click on "My Bar Page"



Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)



If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.

State Bar of Texas Computer & Technology Section Council

COMPUTER AND TECHNOLOGY SECTION