Oregon Business Lawyer

Oregon State Bar Business Law Section Newsletter • September 2019

Choosing a Dance Partner in a Cyber-Connected World

By Dalia Nagati, Corporate Counsel, Tripwire

In-depth cybersecurity due diligence and cybersecurity hygiene must be central to the mergers and acquisitions deal process. In today's connected world, the width of the cyber-attack surface is continually expanding. It therefore is no longer a question of if an organization will experience a cyber breach, but when. Organizations of all sizes are potential targets. In an analysis of 1,201 cyber insurance claims for incidents that occurred between 2013 and 2017, 14% of claims were for organizations with greater than $300 million in annual revenue, and 49% of claims were for organizations with annual revenues of less than $50 million.

Cost of a breach

The cost of a data breach can be staggering and difficult to estimate. Ponemon Institute's 2018 "Cost of a Data Breach" study put the average cost of a lost or stolen record at $244. The study further notes that the cost per lost record barely represents the potential total losses. Other costs can include regulatory fines, harm to reputation and loss of goodwill, credit monitoring costs, business interruption costs that may include tying up executives' time, or delaying upgrades while the effect of a breach is assessed, to name a few.

One of the most costly data breaches to date was the Marriott hack disclosed in November 2018, originating from the Starwood network. Marriott acquired Starwood in 2016 for $13.6 billion. The vulnerability in the Starwood network was exploited in 2014. 383 million customer records were compromised, exposing at least 25 million passport numbers and 8 million payment cards. Both customers and investors sued in response to the breach. Given that the breach falls under the European-wide General Data Protection Rules (GDPR), Marriott may face penalties of up to four percent of its global annual revenue if found to be in breach of the rules. The magnitude of potential damages flowing from data breaches will only grow as states roll out GDPR-like privacy legislation.

Tailoring the Due Diligence Checklist

Effective cybersecurity due diligence must start early in the deal process, in part because that process may prove to be multi-step in nature, and could have a significant impact on the direction of the transaction. Information technology (IT) systems are inherently complex. Counsel is accustomed to adjusting the diligence review in accordance with the structure of the transaction (asset/share sale or merger). Counsel may also customize the inquiry in accordance with the target's data map/inventory, applicable regulations, industry, and the extent to which the target's assets are digital.

Continued on page 2

In this Issue

Cybersecurity

Continued from page 1

Dalia Nagati is a corporate attorney with more than five years of corporate law experience, both in private practice and in-house, predominantly in Canada and the United Arab Emirates. She is currently in-house corporate counsel at cybersecurity software company Tripwire. Her practice areas include software licensing, data privacy, and IP portfolio management.

Nonetheless, the technical experts weighing in early on the questions in the due diligence checklist will prove to be of great benefit. The experts will assist in development of the right diligence inquiries, and know when and how to delve beyond broad requests for documents and general information about policies and practices. Effective due diligence will be achieved when the subject-matter experts are in conversation with one another.

Establishing a Security Committee

Once the buyer has developed the due diligence checklist with input from the technical experts, the buyer should form a security committee comprised of information-security and IT professionals from both the buyer and target (or relevant third-party providers). A security committee will prove invaluable in several ways. Face-to-face meetings and open dialogue provide insight into the target's culture as it relates to risk management practices and accountability. A security committee will also help ensure timely deal closing and a smooth post-closing integration process. The merging or migration of networks alone can be a protracted process that itself may create vulnerabilities. The overall message underlying the creation of a security committee must clearly be one of facilitating the transaction, and value preservation for both the buyer and target. In the event potential security gaps are identified during the course of due diligence, the security committee may be able to develop solutions or mitigate potential issues. Addressing technical issues early and head-on—rather than through laborious and likely contentious adjustments to representations and warranties, indemnification. or even the purchase price—will benefit both sides.

The legal team must enlist and empower the technical subject-matter experts early in the transaction. It is difficult to bring legal clarity to highly technical IT systems. The representations and warranties wind up being somewhat broad and ambiguous. The target will naturally push back and limit the scope of those representations and warranties, with the risk of the final draft being rather opaque. In turn, the disclosure schedules can lack the detail required to bring visibility into the IT systems and any security gaps.

As a result, proving whether the representations and warranties have been breached can be fraught with difficulty. A thorough and well-structured cybersecurity diligence review driven by the security committee can be the most effective step to managing cyber risks.

Cybersecurity Maturity Models

As with data-privacy diligence, there is no single standard, rule, or guideline for assessing an organization's information-security posture. Gaining in popularity among information security professionals is the concept of a cybersecurity maturity model. Several models are available to serve as a baseline framework for assessment of the strengths and weaknesses of a given security program, to essentially determine whether an organization is reactive or proactive in certain key areas. A broadly cast cybersecurity maturity model makes a useful tool to identify cybersecurity risks in a diligence target, and to assess whether an organization's cyber-risk measures are appropriate in light of those risks. The development of such frameworks includes a component of subjectivity. However, a self-assessment provides a means of measurement, which is better than no measurement at all.

Security Culture

In considering and managing cyber risks in the M&A deal process, counsel should keep abreast of the leading causes of cyber breaches. The data-breach bible, Verizon's data-breach incident report, reveals the leading causes of security incidents—physical theft of devices, failure to timely inform IT departments, and privilege misuse—are common examples. Therefore, during the due-diligence process heavy emphasis should be placed on understanding the target's information-security culture. What is the knowledge level of the executives on information-security matters? Does the target have dedicated employees focused on data security and privacy issues? What are the reporting lines for the information-security department? Is the size of the information security/IT department appropriate given the size of the company and breadth of its cyber surface? Is information security discussed at board meetings? What is the nature and frequency of company-wide cyber-awareness training? How does the rate of phish-test failures compare to comparable organizations?

Continued on page 3

Cybersecurity

Continued from page 2

Effective cybersecurity due diligence must start early in the deal process, in part because that process may prove to be multi-step in nature, and could have a significant impact on the direction of the transaction.

Vendor Risk Management

The second leading cause of data breaches relates to vendor risks. The highly publicized breaches suffered by Target and The Home Depot were traced back to network access credentials that were stolen from the third-party HVAC vendors, who were connected to their respective core networks. Due diligence should include a detailed review of the target's vendor risk management program. In addition to assessing the findings of the security committee on the target's vendor risk management program, the contracts of any vendors connected to the target's network must be carefully scrutinized to ensure appropriate contractual protections are in place that address security controls, appropriate indemnification for security incidents, and termination rights.

Verifying the Diligence Response: Penetration Tests

After receipt and evaluation of responses to the due diligence checklist, a cyber risk can be managed during the deal process by implementing penetration tests ("pen tests") or stress tests. The purpose of a pen test is to test the target's public-facing networks to determine whether any doors are inadvertently left open. "Open doors" potentially allow a hacker access to internal networks. The results of pen tests may prove a useful reference point to evaluate the due diligence findings and whether or not the target company's representations stand up to scrutiny. After all, a target's evidence in due diligence can sometimes be aspirational, as opposed to indicative of operational reality. Organizations more frequently find out about a data breach from an outside source (e.g., law enforcement or a security vendor) than internally, with the median time to discover an incident being 146 days.

Responding to Security Gaps

Due diligence may reveal regulatory violations or risks. Depending on the nature and size of the risks or liabilities exposed, and the parties' level of motivation to see the deal close, resolution of cybersecurity or privacy concerns can take a number of forms short of breaking the deal. For example, covenants to remediate the problem, related milestones, and a purchase price holdback may be crafted; or pricing adjustments related to the remediation costs may be negotiated. In the event the target did not carry cybersecurity insurance or carried inadequate coverage, a thorough cybersecurity risk assessment will help move along the typically protracted process inherent in procuring coverage and will likely provide for more favorable policy terms and premiums.

Transactional Security

Finally, M&A lawyers must be prepared to manage risks associated with the release of sensitive data during the due diligence process. Particularly in the case of deals announced at signing, but with closing delayed, the target—and the firms representing both the target and buyer—are especially vulnerable to cyber attacks.

The FBI has reported that law firms— with information on multiple clients—are often viewed as "one-stop shops" for hackers. Law firm breaches have ranged from those resulting from a lost or stolen laptop or mobile device to deep penetration of a law firm network, with access to everything, for a year or more.

Law firms must implement data-security hygiene sufficient to avoid reputation damage and litigation risks. The existence of the deal itself and the target's financials and intellectual property will likely fetch a handsome price. Intellectual property can be a critical element of the deal's value. Information about company employees and vendors can also provide hackers with new targets of phishing and other social engineering attacks. Information about the organization's information-security policies, network architecture, and the security tools in use will also prove highly useful to a cybercriminal. In addition to using an appropriately certified virtual data room, proper policies (both physically written policies and access-control policies) must be in place to control access to deal documents from various devices, including smartphones.

Conclusion

We live in a time where data is cash. Hackers are increasingly sophisticated. Increased regulation is slowly rolling in. The stakes are high. The traditional composition of the deal team, and the traditional approach to due diligence and managing data security risk by which counsel and financial executives work together, are well worth careful reassessment. ◆

Understanding and Preparing for the California Consumer Privacy Act of 2018

By Eric Beach and Parna Mehrbani, Tonkon Torp LLP

Eric Beach is a member of Tonkon Torp's intellectual property and entrepreneurial services practice groups, He focuses his practice on intellectual property, creating and negotiating technology and software licenses, and protecting clients' trademark, patent, copyright, and trade secret rights through litigation in both federal and state court.

Parna Mehrbani is a partner at Tonkon Torp. Her practice is focused on intellectual property, trademark registration and enforcement, and advising and litigating trademark portfolios for local, national, and international companies at all stages of growth.

As you may know, the United States traditionally has lagged behind other countries in regulating individual privacy rights in personal information. This became apparent in 2018 when the European Union's General Data Protection Regulation (GDPR) went into effect, causing confusion and concern for businesses in the United States and around the world. California recently enacted a comprehensive data privacy statute, the California Consumer Privacy Act of 2018 (CCPA). The CCPA will go into effect on January 1, 2020, establishing broad privacy rights for California residents ("consumers" in the CCPA) over how their personal information is collected, used, and sold by businesses. The CCPA will have a significant effect on businesses across the country, not just those based in California.

The CCPA defines "personal information" more broadly than in any prior privacy statute in the United States and more broadly than in the GDPR. In the CCPA, "personal information" includes any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Beyond the data one would expect to be personal information, (names, addresses, Social Security numbers, and account numbers), it also includes items that indirectly identify a unique person, such as aliases, IP addresses, browsing history, commercial/purchase history, geo-location information, and biometric information.

The CCPA applies to any for-profit business, regardless of location, that does business in California, either collects personal information or determines the purpose and means of processing personal information relating to a consumer, and satisfies any one of the following three thresholds:

- annual gross revenues in excess of $25 million (total, not just in California)
- annually, either alone or in combination, buys, receives, sells, or shares for commercial purposes the personal information of 50,000 or more consumers
- 50% or more of its annual revenues result from selling personal information of consumers

Many businesses not based in California may believe the CCPA will not apply to them. However, simply having 137 California residents a day access a company website and collecting information from those visitors satisfies the second threshold noted above. Additionally, as you may have experienced with the GDPR, even if a client's business does not meet one of these thresholds, customers, vendors, or other business partners who are subject to the CCPA may require that your clients comply with the CCPA by agreement.

The CCPA imposes substantial obligations that require businesses, at or before the point of collecting personal information from a consumer, to notify the consumer of the categories of personal information that will be collected and the purposes for which that personal information will be used.

The CCPA also gives consumers the right to request disclosure of the personal information a business has collected about them in the previous 12 months, the categories of sources of that personal information, the business purposes for collecting or selling that personal information, and the categories of third parties with whom that personal information is shared. Subject to a number of exceptions, consumers may also request deletion of their personal information.

As of January 1, 2020, a business subject to the CCPA must be prepared to provide a complete and accurate response to a consumer request for disclosure, including all the responsive information for the preceding 12-month period—that is, dating back to January 1, 2019. Such responses must be provided free of charge and within 45 days (which may be extended in certain circumstances).

If a business sells personal information, it is also required to have a clear and conspicuous "Do Not Sell My Personal Information" link on its website leading to a page that enables consumers to opt out of the sale of their personal information.

Continued on page 5

California Consumer Privacy Act *Continued from page 4*

The CCPA will have a significant effect on businesses across the country, not just those based in California.

For minors, an affirmative opt-in is required before a business can sell personal information of those between the ages of 13 and 16, and parental opt-in is required for minors under the age of 13. (These are in addition to the already-existing requirements of the Children's Online Privacy Protection Act). These opt-out and opt-in rights are bolstered by the CCPA's very broad definition of "sell,"which encompasses "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information … for monetary or other valuable consideration." In short, "selling" is more than just cash for information exchanges, and includes any transfer for value.

The CCPA will be enforced by the California Attorney General, with statutory penalties up to $7,500 per violation. A private right of action exists in cases of breach of non-encrypted or non-redacted personal information (with a narrower definition of "personal information" in this context). There is also some concern that enterprising attorneys will attempt to bring additional private actions or class actions by using the CCPA's requirements in connection with unfair-trade-practices claims.

These and the other rights and requirements created by the CCPA are subject to further detail, and a number of exceptions. Moreover, many potential amendments are currently pending in the California legislature, and the California Attorney General's rule-making deadline is not until July 2020. Despite compliance being somewhat of a moving target, given the substantial obligations imposed by the CCPA, businesses should begin preparing to comply now.

Businesses must first understand what personal information they collect, and how and why such data is used, disclosed, or sold. They will then need policies and notices that reflect their collection, use, and disclosure. They must review agreements that concern disclosure and use of personal information and make appropriate security updates to address potential vulnerabilities. Finally, businesses should begin creating protocols and training personnel to respond to consumer requests under the CCPA.

Due to many recent high-profile cases and proceedings concerning consumer privacy and data security, privacy concerns are becoming a primary concern of consumers, businesses, and government officials. The CCPA is only the first in what will be a series of data-privacy laws implemented at the state and federal levels. Businesses that begin preparation now will not only be prepared for the CCPA, but ahead of the curve in regard to future privacy laws and consumer expectations of privacy. ◆

New FCC Rules Focus on Phone Scams

On May 23, 2019, the U.S. Senate overwhelmingly approved the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act by a 97-1 vote.

The bill gives the federal government the authority to slap offenders with fines of up to $10,000 per call. The legislation also gives regulators more time to find scammers, increase penalties for those who are caught, promote call authentication and blocking, and help coordinate enforcement to increase criminal prosecution of illegal robocallers.

In addition, on June 6, 2019, the FCC voted unanimously to grant telecommunications companies the authority to proactively identify and block robocallers. The agency has committed to pursuing "aggressive enforcement action" against illegal robocallers.

According to call-protection company First Orion, which analyzed data from 50 billion calls over 18 months, the percentage of spam phone calls has jumped from 3.7% of total calls in 2017 to 29.2% in 2018—and it predicts that number will rise to 50% by year end. ◆

New Statute Allows Corporations to Ratify Defective Corporate Actions

By Justin Denton, Tonkon Torp LLP, and David Ludwig, Farleigh Wada Witt

While preparing a legal opinion required by your client's lender, you find that the borrowing corporation has issued more shares than its articles of incorporation authorize. After scouring the corporation's minutes book, you are not satisfied that any subsequent corporate action taken by the shareholders was valid, including electing the current board of directors. Are you willing to creatively "fix" the problem and put your firm's malpractice policy on the line by opining that the loan transaction is properly authorized?

Historically, Oregon had no statutory procedure to correct defective corporate actions. A corporate action that is not properly authorized could be invalid. An Oregon corporation's directors or shareholders may wish to fix invalid corporate actions by later ratifying them. However, Oregon courts have not clearly distinguished between defective corporate actions that are "voidable" (capable of being cured) and those that are void (incapable of cure). Oregon law is also unclear how to effectively cure voidable actions.

Earlier this year, Governor Brown signed into law Senate Bill 359, which expressly permits ratifying many defective corporate actions. This new law, which is based on a recent addition to the Model Business Corporation Act, clarifies what defective corporate actions may be cured, and describes how to properly ratify those defective actions.

Here are a few highlights of the new law:

1. Effective January 1, 2020, it amends the Oregon Business Corporation Act and the Oregon Nonprofit Corporation Act.
2. It does not exclude or limit ratifying defective corporate actions by using common law or other approaches.
3. It allows ratifying defective actions that were purportedly taken by the corporation's incorporator, board of directors, officers, agents, or any other person acting on the corporation's behalf.
4. It permits ratifying only defective actions that (a) are currently within the corporation's power to take, and (b) were within the corporation's power to take when the corporation originally took the defective action.
5. To effectively ratify a defective corporate action, the corporation's:

(a) Board of directors must ratify the action by satisfying the same quorum and voting requirements that applied at the time the defective action was originally taken; and

(b) Shareholders must approve the board of director's ratification if the defective action (i) currently requires shareholder approval or (ii) would have required shareholder approval on the date the defective action was originally taken.

6. If shareholder approval of the board's ratification was not required, all current shareholders, and certain former shareholders who owned shares when the defective corporate action was originally taken, must be notified in writing that the board ratified the defective action.
7. Once a defective corporate action is properly ratified under this law, the corrected action is effective as of the date the original defective corporate action took place.
8. If a defective corporate action results from, or is taken in reliance on, a previous defective corporate action, the later act is valid and effective when the previous action is properly ratified under this law.
9. In some circumstances, the corporation must also file "articles of validation" with the Oregon Secretary of State. Articles of validation become part of the corporation's public filings. These articles must describe the defective corporate action, specify why proper authorization failed, and state that the corporation's board ratified the defective corporation action and, if applicable, that the shareholders approved the ratification. When filed, articles of validation amend, supplement or replace, as appropriate, any previous filing with respect to the defective corporate action. This law may also require the corporation to file an amendment to its Articles of Incorporation.
10. Only certain parties may bring an action claiming that the ratification under this law is not effective, or that it is effective only under certain conditions. Those claims must be brought in state court within 120 days after a defective corporate action is validated and the shareholders are properly notified.

This new law offers a safe harbor to Oregon corporations needing to correct past defective actions and the consequences those actions produce. Although its procedures are detailed and exacting, carefully applying this new law can assure certainty and finality for our Oregon corporate clients. ◆

Business Law Section News

Subcommittee Reports

Continuing Legal Education

The Business Law Section's annual CLE seminar, co-sponsored by the Oregon State Bar, will take place Friday, November 8, 2019, at the Multnomah Athletic Club in Portland. The seminar, "Refreshing the Old and Learning What's New – Practical Updates for Business Lawyers," will feature multiple presentations on topics such as intellectual property, secured transactions, contract drafting, representation and warranty insurance, and securities regulations, and will include an ethics CLE. Watch for registration information from the Bar.

The planned topics:

- Seven Ways to Identify and Protect a Company's Intellectual Property
- Codes of Conduct and Building a Culture of Compliance: a View from the Inside
- Ethics for Business Lawyers
- Secured Transactions for Business Lawyers
- Tips for Clear and Effective Contract Drafting
- Securities Regulation Refresher
- R & W Insurance: a (Relatively) New Tool in the M&A Toolbox
- Using Technology in Your Law Practice: Today and Tomorrow
- SB 359: Ratification of Defective Corporate Actions
- What Business Lawyers Need to Know About Fixing Past Tax Errors

Do you have ideas for a business law CLE program? Please contact CLE subcommittee chair Kara Tatman at ktatman@perkinscoie.com.

New Business Lawyers

This subcommittee meets monthly and its members participate in working groups that focus on education, social events, law schools, and newsletter participation. If you would like to be involved with the subcommittee or its activities, please reach out to the subcommittee's chair, Will Goodling of Stoel Rives LLP at (503) 294-9501 or william.goodling@stoel.com.

On July 20, 2019, the New Business Lawyers Subcommitee co-hosted a summer picnic at Laurelhurst Park with the Oregon New Lawyers Division.

New Lawyer Mentoring Program

In 2011, the Oregon Supreme Court instituted the New Lawyer Mentoring Program. All new OSB members are required to complete the program in their first 12–18 months as members.

Attorney Mark Wada says, "I have been a mentor in the OSB's mentoring program for new lawyers on two occasions. Participating in this program as a mentor gives you an opportunity to share your experience, battle scars, mistakes, triumphs, and insights, which will give new lawyers a valuable perspective on everything from the nuts and bolts of practicing law, ethical and professional responsibilities, to the role lawyers play in the justice system and our community."

To serve as a mentor, an attorney must be a member of the OSB in good standing, have at least five years' experience in the practice of law, have a reputation for competence and ethical and professional conduct, have no current disciplinary prosecutions pending, and be appointed by the Oregon Supreme Court.

The typical time commitment is a monthly 90-minute meeting for 12–18 months. At the completion of the program, the mentor receives eight CLE credits, including two ethics credits.

For a quick "At-a-Glance" summary of the program, click here: http://www.osbar.org/_docs/NLMP/NLMPAtAGlance.pdf

For more complete information and to enroll as a mentor, click here: https://www.osbar.org/nlmp/index.html

Please email questions to mentoring@osbar.org or reach the program coordinator, Cathy Petrecca, at (503) 431-6355. ◆

Nominations due for James B. Castles Leadership Award

The Business Law Section of the Oregon State Bar is seeking nominations for the James B. Castles Leadership Award.

The award was established in 1998 to recognize an Oregon lawyer for excellence in the practice of business law, professionalism among fellow business lawyers, and outstanding community leadership. It is the highest recognition that the Business Law Section can bestow on one of its members.

James B. Castles began his career as an Oregon business lawyer advising Tektronix, Inc., founders Jack Murdock and Howard Vollum in the start-up phases of their business. He subsequently became the founding General Counsel of Tektronix and a long-time director of the company. Mr. Castles was also well known for his philanthropic support of Northwest organizations, and served as a founding trustee of the M. J. Murdock Charitable Trust.

Previous recipients of the James B. Castles Leadership Award include Otto B. Frohnmayer, Henry H. Hewitt, Brian Booth, Andrew J. Morrow, Jr., Donald L. Krahmer, Jr., Neva Campbell, Robert Art, MardiLyn Saathoff, John Jaqua, Ruth Beyer, Brent Bullock, Carmen Calzacorta, Kenneth D. Stephens, Jeffrey C. Wolfstone, and John M. McGuigan.

Candidate Qualifications

To be considered for the James B. Castles Award:

1. The nominee must be a licensed (or retired) member of the Oregon State Bar, recognized for excellence and professionalism;
2. A significant portion of the nominee's career must have involved the practice or teaching of business law; and
3. The nominee must have shown outstanding community leadership in one or more of the following areas:
   a. Activities supporting other members of the Oregon State Bar in the practice of business law, such as serving on committees or task forces of the Business Law Section or other business-law-related committees or task forces, serving on the Board of Governors, writing business-law related articles or treatises, teaching-CLEs, and other similar activities;
   b. Civic leadership, such as serving on public boards or commissions, as a member of federal, state, regional, county, or local government, or as an employee of the Department of Justice or a state agency, or otherwise having been elected or appointed to public office; or
   c. Business or non-profit leadership in community affairs or economic development, such as serving with one or more nonprofit organizations engaged in community development, economic development, or charitable activities.

Nomination Procedure

If you would like to nominate an Oregon business lawyer for the James B. Castles Leadership Award, please send the name of the nominee, together with the pertinent details regarding the nominee's qualifications for the award, to David R. Ludwig at dludwig@fwwlaw.com.

The deadline for nominations is October 11, 2019.

Nominations will be reviewed by the 2019 James B. Castles Award Committee, consisting of past chairs of the Business Law Section.

Following that review, the Award Committee will determine whether to make a recommendation to the Executive Committee of the Business Law Section for final selection.

The 2019 James B. Castles Leadership Award will be presented at the lunch during the Business Law Section's annual CLE pogram on November 8, 2019. ◆

Oregon State Bar Business Law Section

The mission of the Oregon State Bar Business Law Section is to provide excellent service to the diverse group of business-law practitioners throughout the State of Oregon by providing regular, timely, and useful information about the practice of business law, promoting good business lawyering and professionalism, fostering communication and networking among our members, advocating improvement of business law, and supporting Oregon's business infrastructure and business community.

Upcoming Events

CLE Programs

Legal Issues for Growers Using the H-2A Program
Thursday, September 19, 2019/12:00–1:00 p.m.
Dunn Carney
851 SW Sixth Ave., Suite 1500, Portland
Sponsored by The Agricultural Law Section

Broadbrush Taxation: Tax Law for Non-Tax Lawyers
Thursday, October 3, 2019/9:00 a.m.–4:45 p.m.
Oregon State Bar Center/Tigard
Cosponsored by the Taxation Section

Oregon Legislative Update
Wednesday, October 16, 2019/12:00–1:00 p.m.
Red Star Tavern, 503 SW Alder St., Portland
Sponsored by the Taxation Section

Don't Lose for Winning: Identifying and Avoiding Settlement Pitfalls
Friday, October 25, 2019/ 9:00 a.m.–5:00 p.m.
Oregon State Bar Center, Tigard
Sponsored by the Consumer Law Section

The Corporate Designee Deposition: Avoiding Traps & Pitfalls
Thursday, November 7, 2019/12:00–1:00 p.m
Standard Insurance, Auditorium
900 SW Fifth Ave., Portland
Part of the Multnomah Bar Association Advanced Pre-Trial Litigation Series

Refreshing the Old and Learning What's New: Practical Updates for Business Lawyers
Friday, November 8, 2019/all day
Multnomah Athletic Club, Portland
Business Law Section annual CLE program
See page 7 for more information.

Social Event

Oregon State Bar Annual Awards Luncheon
Friday, November 15, 2019/11:30 a.m.–1:00 p.m.
The Sentinel Hotel
614 SW 11th Ave., Portland

Based on nominations from members and the public, the Oregon State Bar honors a select group of lawyers and judges who have made outstanding contributions to the community and the profession.

Job Postings

Land Use Attorney. Tomasi Salyer Martin PC is a 9-lawyer, dynamic law firm in downtown Portland, with a strong commitment to providing excellent services to our land use, financial institution, and business clients, while enjoying a balanced life in the Pacific Northwest.

We seek a land use attorney with at least three years of meaningful land use experience, including preparation of briefs, permitting documents, and client advocacy before various tribunals. You will have the opportunity to work on complex land use cases, participate in hearings, and argue cases.

Strong research and writing skills are required. Must be licensed with the Oregon State Bar and admittance in Washington is a plus. We strongly value congeniality and teamwork among all our employees, and strive to think "outside the box" in our business model. We have been a majority women-owned firm since we opened our doors in 2012, and support diversity in our hiring discussions.

Interested applicants should send their resumes and cover letters to jcharles@tomasilegal.com.

Experienced Corporate/M&A Attorney. Rose Law Firm is a 7+ attorney business-focused law firm in Lake Oswego. We seek an attorney with 15+ years of experience in handling complex corporate/commercial transactions and associated client engagements—including file and team management. Position is ideal for someone who wants to transition away from the billable-hour demands of a larger firm but is still interested in maintaining a sophisticated practice and collabo,rating with a team of like-minded professionals.

If you bring a partial book of business, that is great, but not necessary. This position requires someone with: (a) strong experience and an exceptional substantive corporate law/M&A skillset; and (b) a desire to contribute to helping Rose Law thrive and expand. We offer competitive wages and benefits (health, dental, vision, life, 401(k)) and can be flexible with billable hour goals (between 1,200 –1,800). Culture is very important: we take our work seriously, but do not take ourselves too seriously. Large egos don't function well here.

To apply, send cover letter, resume, and references to Crystal Hutchens, chutchens@rose-law.com. For more details, please review: https://www.rose-law.com/careers.

Brix Law LLP is seeking a Lateral Partner/Senior Associate and a Junior Associate or experienced paralegal to join our Bend office. We are a specialized law firm with offices in Portland and Bend focused on real estate, corporate, and land use transactions, looking for the right person to join us. Our firm culture is business-minded, responsive, and practical in our approach to our clients' needs, whether working on complex, sophisticated transactions or more routine matters.

Our strength lies in teamwork, providing legal advice to capture the entirety of our clients' land use, real estate, and corporate transactional needs. If you have experience in one of these areas, are able to work hard and play hard, then we might be the right firm for you. We also value responsiveness, attention to detail, excellent analytical and critical thinking skills, written communication skills consistent with that of a top-tier law firm, a good work ethic and a sense of humor.

Please send cover letter and resu,me to Holly Gullickson at hgullickson@brixlaw.com. All inquiries will remain confidential.