



Independent Contractors versus Employees: The Latest from the Oregon Supreme Court

By Nicole Elgin

The question of whether a person qualifies as an independent contractor versus an employee is an increasingly important one in the rise of the “gig economy.” For business owners, it can also be an expensive question to get wrong, considering the various taxes, insurance, and benefits – not to mention the penalties – that a business owner might owe if the state determines that what the business called “contractors” are actually “employees.”

As recently as May 2018, the Oregon Supreme Court weighed in on the test for determining whether an individual qualifies as an independent contractor for purposes of unemployment insurance tax in *ACN Opportunity, LLC v. Employment Department*, 362 Or 824 (2018). ACN Opportunity sold satellite-television, telephone, Internet, and home-security services, as well as other items related to those services. The company used a network of direct-to-consumer sellers that it called “independent business owners.”

In auditing the company, Oregon’s Employment Department found that the company was an employer, and therefore required to pay unemployment-insurance tax on the earnings the company paid to the independent business owners for their sales. On appeal, the Oregon Supreme Court addressed the statutory interpretation questions and affirmed that the independent business owners were not independent contractors.

Nicole Elgin is a labor and employment attorney with Barran Liebman LLP.



Professional Liability Fund

inBRIEF IS PUBLISHED BY

The Professional Liability Fund

Carol J. Bernick
Chief Executive Officer

EDITORS

Tanya Hanson,
Loss Prevention Attorney
tanyah@osbplf.org

and

Barbara S. Fishleder,
Director of Personal and Practice
Management Assistance

phone: 503.639.6911
toll-free: 1.800.452.1639
www.osbplf.org

**PROFESSIONAL LIABILITY FUND
BOARD OF DIRECTORS AND OFFICERS**

Saville W. Easley
Portland
Chair

Molly Jo Mullen
Portland
Vice Chair

Tom Newhouse
Portland
Secretary-Treasurer, Public Member

Robert S. Raschio
Canyon City

Holly N. Mitchell
Portland

Megan I. Livermore
Eugene

Susan Marmaduke
Portland

Gina Anne Johnnie
Salem

Patrick Hocking
Medford
Public Member

TABLE of CONTENTS

LAW UPDATES

Independent Contractors versus Employees: The Latest from the Oregon Supreme Court..... 1

File and Serve Support Modifications Before Termination of Spousal Support Obligation 6

Securities Liability for Transactional Lawyers: The Blues of Oregon’s Blue Sky Law 7

Cases of Note 12

PLF UPDATES

Message from the CEO..... 3

PLF Board of Director Positions..... 3

2018 PLF Annual Report Now Available 4

LAW PRACTICE

Cybersecurity and Employee Training..... 9

DISCLAIMER

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics presented. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund except that permission is granted for Oregon lawyers to use and modify these materials in their own practices. © 2019 OSB Professional Liability Fund.

Message from the CEO

By Carol J. Bernick, PLF Chief Executive Officer

THE PEN IS MIGHTIER THAN THE BLANK PIECE OF PAPER.

After five years of reviewing claims – big and small – one of the most frequently occurring problems is the absence of clear communication to the client. Those communications can be in an email or letter to the client or even a memo to the file (less ideal) documenting the advice given. Whether it's advice about a business strategy, an estate planning strategy or a litigation strategy, write it down. Explain the options and the consequences for the options, then confirm the client's decision. This can be hard to do when things are moving quickly, which is why email can be an effective strategy. In short, no claims attorney who receives your file after a claim has been made has said, "I wish there were fewer communications with the client in here."

THE PLF IS A SAFE SPACE.

If you need help, call. The practice management advisors, claims attorneys, and OAAP attorney counselors all fill different roles, but they each share the same mission: to help you serve your clients at the highest level. A legal career is rewarding, but it can be arduous and overwhelming at times. If you

fear you have made a mistake or when you need help to get your practice or your life on track, the PLF can help. Use us and use the myriad resources on our website. Your communications with the PLF are confidential. www.osbplf.org

CONSIDER EXCESS COVERAGE.

Look at the types of work you do and the amounts at issue. If it exceeds \$300,000 in a year, you are exposing your personal assets if you do not have additional coverage to protect against a larger claim.

HAVE BACK-UP.

Half the lawyers in private practice are solo practitioners. Consider designating someone to be your back-up person in the event unforeseen circumstances take you away from your practice for an extended period of time. Too often we see a sudden illness create claims that may have been avoided if the lawyer had pre-arranged for someone to assist in time of need. The practice management advisors can help you do this. And bonus prize: Those solo lawyers who have a designated back-up person receive a discount on their PLF Excess coverage.

PLF Board of Director Positions

The Professional Liability Fund is looking for two lawyers, each to serve a five-year term on the PLF Board of Directors beginning January 1, 2020. Directors attend approximately six board meetings per year, plus occasional committee meetings. Directors are also required to spend time reading board materials and participate in occasional telephone conferences between meetings. PLF policies prohibit directors and their firms from prosecuting or defending claims against lawyers. The PLF Board recognizes that Bar members are diverse

in perspective and background; we highly encourage individuals from a diverse background to apply.

Interested persons should send a brief resume by July 8, 2019, to:

Carol J. Bernick
carolb@osbplf.org
 Professional Liability Fund
 PO Box 231600
 Tigard, OR 97281-1600

2018 PLF Annual Report Now Available

The 2018 PLF Annual Report is now available. Go to www.osbplf.org > [About PLF](#) > [Annual Reports](#).

LAW UPDATES

INDEPENDENT CONTRACTORS VERSUS EMPLOYEES (CONTINUED FROM PAGE 1)

To understand the court's legal analysis, it is important to know the facts surrounding the nature of the relationship between ACN and the independent business owners, which was governed by a written contract. The contract between ACN and the sellers stated that each seller agreed to pay ACN an initial fee for a one-year license to sell ACN products and could pay a renewal fee each year. The contract also specifically stated that the sellers would sell ACN's products as "an independent contractor," not as an employee, and that sellers received commissions and bonuses from ACN from selling the product and getting new customers' subscriptions. The contract also restricted the sellers' marketing, prohibiting "cold marketing" techniques like trade shows, door-to-door sales, and pamphlet distribution.

After paying the initial fee, the sellers received a "Team Trainer Kit" and access to ACN's customer tracking services, ACN's website to submit customer orders, and ACN's back office and call center services. ACN did not provide computers, telephones, training, or marketing materials, but those items could be purchased from ACN. The contracts allowed the sellers to choose where and how many hours to work, as ACN did not offer office space to the sellers and ACN did not even have an office in Oregon. The Oregon sellers worked out of various locations, including coffee shops, hotel conference rooms, and the homes and offices of their customers.

The court's analysis first reminded business owners that, "for purposes of unemployment insurance tax liability, Oregon law begins with the presumption that a person who performs services for remuneration is an employee, and the employer must pay

unemployment-insurance taxes on that person's wages." *Id.* at 826-27. In explaining the presumption, the court cited ORS 657.505(2), which reads that "an employer shall be liable for taxes on all wages paid for services performed on or after the first day of a calendar quarter." Thus, to avoid unemployment insurance tax liability, a business owner must prove that the worker is an independent contractor under ORS 670.600 or qualifies for one of the exemptions from "employment" under ORS 657.087.

First, the court analyzed ORS 670.600, which provides: "independent contractor means a person who provides services for remuneration and who, in the provision of the services:

Is free from direction and control over the means and manner of providing the services, subject only to the right of the person for whom the services are provided to specify the desired results;

...is customarily engaged in an independently established business;

Is licensed under ORS chapter 671 or 701 if the person provides services for which a license is required under ORS chapter 671 or 701; and

Is responsible for obtaining other licenses or certificates necessary to provide the services."

The court found that the company's independent business owners failed the "customarily engaged in an independently established business" factor of the test because the sellers did not "maintain a business location." 362 Or at 838; ORS 670.600(3) (a). Specifically, the court reasoned that to maintain

a business location, the contractor “must take some affirmative action – more than, for example, temporarily occupying a table at a coffee shop.” 362 Or at 836. Additionally, the court highlighted that the independent business owners did not have sufficient authority to hire others to provide the services, which is another important factor to the independent contractor test. *Id.* at 842; ORS 670.600(3)(e).

The court then looked to the “in-home sales” exemption in ORS 657.087(2): “Employment does not include service performed: ...By individuals to the extent that the compensation consists of commissions, overrides or a share of the profit realized on orders solicited or sales resulting from the in-person solicitation of orders for and making sales of consumer goods in the home.” This exemption was found only to apply to those sales made “in the home,” basing its reading and legislative history analysis on the Tupperware business model. 362 Or at 843-46. Following this application, the exemption could not apply to all of the sellers’ work because they sometimes worked in other locations, such as coffee shops or customers’ offices. *Id.* at 846. Because the company did not meet its burden to prove that the sellers were independent contractors or that they qualified for the employment exemption for in-home sales, the court upheld the Employment Department’s assessment against the company for unemployment insurance taxes.

Those surprised by some of the court’s application of the statutory language to the realities of the modern-day workforce are not alone. In his concurring opinion, Judge Thomas Balmer agreed with the majority’s holding, but urged the Oregon Legislature “to consider revising some of the many statutes that regulate the relationships between those who perform work and those individuals or businesses who pay them, in light of the far-reaching changes that have occurred in the workplace and in the economy over the last two decades.” *Id.* at 847. Reflecting on the increasingly mobile and flexible nature of the growing “gig economy,” Judge Balmer concluded that “it is apparent that existing statutes and regulations do

not address the realities of important parts of today’s work environment.” *Id.* at 850.

This case has several good takeaways for lawyers who advise Oregon business owners on independent-contractor tests:

There are many state and federal “independent contractor” tests, including ones for unemployment insurance, workers compensation, and wage-and-hour laws;

It is almost always the company’s burden to show that the worker is not an employee and does qualify as an independent contractor; and

Each case is highly fact-specific, requiring an attorney to know many details of its client’s operations in order to give the best advice on whether a worker qualifies as an independent contractor.

This article, authored by Barran Liebman attorney Nicole Elgin, was originally published in the September 2018 issue of Oregon Business Lawyer, the newsletter of the Oregon State Bar Business Law Section. Reprinted with permission.

File and Serve Support Modifications Before Termination of Spousal Support Obligation

By Wendy S. Fay

The court lacks authority to modify a support judgment if the motion for modification is not filed and served before termination of the support obligation.

ORS 107.135(1)(a) provides that the court may, at any time after a judgment of annulment or dissolution of marriage or of separation is granted, upon the motion of either party and after service of notice on the other party, set aside, alter, or modify any portion of the judgment that provides for spousal support.

Prior case law has interpreted the statute to require that a motion to modify must be filed before termination of the support obligation. Motions filed after termination were barred. *Wrench and Wrench*, 98 Or App 352 (1989), rev den, 308 Or 608 (1989) (holding that modification filed after the last payment was due was barred). *Harkins and Harkins*, 200 Or App 468 (2005), rev den, 340 Or 672 (2006) (holding that modification filed after prepayment of final support installment, but before the last payment due date, was barred).

A more recent Oregon Court of Appeals case held that a motion to modify support must be both filed and served prior to termination of the support obligation. *Stansell and Stansell*, 295 Or App 224 (2018).

In *Stansell*, husband was required to pay support through August 2016. Wife filed a motion to modify support on July 26, 2016. Husband made his final support payment on August 1, 2016. Husband was served with the motion to modify on August 13, 2016. At trial, the court granted wife's motion to extend the term of support. Husband appealed, arguing that the trial court lacked authority to modify the judgment because his obligation

terminated on August 1, when he made his final support payment, before he was served. Wife argued that under *Park and Park*, 43 Or App 367 (1979), she was only obligated to file the motion before termination, not serve it. The Court of Appeals disagreed with wife's interpretation of *Park*. The court clarified that filing before termination was a necessary, but not sufficient, condition for the motion to be timely. The Court of Appeals agreed with husband holding that a support obligation must exist at the time the motion is filed and served for the court to have authority to modify. Husband's support obligation terminated on August 1 when he made the final payment. Husband was not served until August 13. Therefore, at the time the motion was filed and served, no support obligation existed for the court to modify.

The court in *Stansell* did not reach the question of whether the court must rule on the motion to modify before the obligation terminates for the motion to be timely. *Id.* at 227 n 4.

Attorneys should be mindful of the above time bars. A motion to modify must be filed and served before the last payment due date and before the support obligation has been paid in full. As the date of termination approaches, savvy obligors may pay off their support obligations early to preclude an obligee from seeking a modification. Further, the court in *Stansell* did not address whether the court must also rule on the motion before termination. An attorney representing the obligee who wishes to extend the duration of support should file a motion to modify as soon as the substantial change of circumstances is known.

Wendy S. Fay is an attorney with Zimmer, Bond, Fay & Overlund LLC.

Securities Liability for Transactional Lawyers: The Blues of Oregon's Blue Sky Law

By Dan Keppler

Your real estate client wants to bring in a few “money people” to purchase the property for a new apartment building. Or your small business client needs cash to open another retail location and is getting financing from friends and family.

Ordinary business deals can inadvertently morph into securities transactions whenever somebody puts money into a business, especially if the investors aren't engaged in running the business. And if your client's deal involves the sale of a security, you as the lawyer can incur a significant liability risk if the business fails, even if you competently drafted the deal documents.

The Oregon Securities Law is unique among state “blue sky” securities laws because it imposes liability in favor of the purchaser of a security against “every person who participates or materially aids” in the unlawful sale of a security. ORS 59.115(3). That “person” can include the lawyers who documented the transaction.

Hard to believe? Read *Prince v. Brydon* 307 Or. 146 (1988). The Oregon Supreme Court ruled that a lawyer who prepares documents that supported the unlawful sale of securities may be held liable under the statute where the documents are material to the sale. Disgruntled investors may rely on *Prince* to argue that they can establish a lawyer's liability even if the lawyer did not know about the facts that made the sale of securities unlawful.

So how can you understand your risk if you don't practice securities law? Here are three questions to consider:

DOES MY CLIENT'S DEAL INVOLVE A SALE OF SECURITIES?

The definition section of the Oregon Securities Law, ORS 59.015 (19), contains a laundry list of things that constitute securities. Not only does this list include classic securities like stocks and bonds, but it also includes promissory notes in many circumstances. See *Lahn v. Vaisport*, 276 Or App 468, 483 (2016).

CONTINUED ON PAGE 8

Dan Keppler is an attorney with Garvey Schubert Barer.

Most importantly, the definition of security includes a catchall for “investment contracts.” An investment contract has four attributes: (1) an investment of money or money’s worth; (2) in a common enterprise; (3) for profit; and (4) to be achieved by the management or control of others. *Computer Concepts, Inc. v. Brandt*, 310 Or 706, 714 (1990).

LLC memberships, partnerships, or real property tenant-in-common interests can all constitute securities if they meet this four-part test. A good rule of thumb is, if your deal involves investors who aren’t actively involved in running the business, those passive investors are likely being sold a security.

CAN MY CLIENT BE POTENTIALLY LIABLE AS THE SELLER OF SECURITIES?

The issuer or seller of securities is liable to the purchaser for any violation of the Oregon Securities Law. Two types of violations are commonly alleged against the seller in securities litigation under the statute:

(1) The seller failed to comply with the technical requirements of the Oregon Securities Law or implementing regulations. ORS 59.115(1)(a). A common violation is the failure to register the security with state regulators or failure to qualify for an exemption from registration. See ORS 59.055 (requiring securities to be registered or exempt).

(2) The seller sold the security by means of an untrue statement of material fact or misleading omission. ORS 59.115(1)(b). The damages for seller liability are the entire amount the purchaser invested, plus interest at the nine percent statutory rate, plus court-awarded attorney fees. ORS 59.115(2).

AS THE LAWYER, COULD I BE LIABLE AS A “NONSELLER” OF SECURITIES?

If the seller or issuer of securities (i.e., your business client) is liable for an unlawful sale, then the Oregon Securities Law imposes liability on certain categories of “nonsellers” involved with the sale. Potentially

liable nonsellers include managers, officers, directors, and others who controlled the seller (i.e., your client’s management team). But it also includes any person who participated and materially aided in the unlawful sale of securities. ORS 59.115(3).

This could include you as the lawyer who drafted the deal documents or advised the business client — if your work can be said to have materially aided the sale of the securities. And, a disgruntled investor need not prove you knew about the facts that made the sale of securities unlawful. *Prince*, 307 Or at 150. Instead, to escape liability, you bear the burden to prove at trial that you did not know, or in the exercise of reasonable care could not have known, about the facts that made the sale unlawful. See ORS 59.115(3).

So what can you do as a business or transactional lawyer to avoid the risk of securities liability? For starters, choose your clients and deals carefully. Avoid clients who might take advantage of unsophisticated investors or are unwilling to be transparent about the risky nature of investing in a business. Also, avoid doing the legal work on deals that seem unrealistic or destined to fail.

If you’re not well versed in securities, avoid getting involved in transactions with passive investors. Try to limit the scope of your representation to matters unconnected to the financing portion of the transaction or to the sale of any securities. If you think you have a securities issue, bring in experienced securities counsel.

Unfortunately, there are no safe harbors, no best practices, and no agreed-upon standards of care for mitigating risks under the Oregon Securities Law. But if you understand and identify the risks, you are more likely to avoid them.

Cybersecurity and Employee Training

By Rachel Edwards, PLF Practice Management Advisor

An important part of reducing your firm's risk of a cyberattack is proper employee training. According to Verizon's 2018 Data Breach Investigations Report, phishing or other forms of social engineering, which are defined as fraudulent attempts through manipulation in order to obtain sensitive information, cause 93% of all data breaches. Firm employers must make it clear to employees the importance of cybersecurity. Listed below are general tips for implementing cybersecurity employee training:

- **Require social engineering awareness training.** Social engineering is defined as the act of gaining access to buildings, systems, or data by manipulation and exploitation of human psychology rather than physically breaking in or using hacking capabilities. Social engineering awareness training develops awareness of ways that you can be exploited, such as phishing scams or people posing as vendors.
- **Create written security policies.** Update these policies regularly, and require all employees to review them upon hiring, annually, and after any change to the policies. Below are specific policies you may consider including:
 - *Use of firm technology.* Employees are prohibited from using technology resources provided by the firm, including Internet and email access for personal use.
 - *Malware protection.* Require all employees to use malware protection software.
 - *Protection of firm devices.* Require devices containing client data to be password protected and encrypted, especially if the device is taken offsite. Prohibit employees from leaving devices in their vehicle, even in a locked trunk. If employees travel for work-related activities, consider requiring employees to store the device in a safe in their room or at the hotel front desk. Also consider using a program that can track the location of a device and erase its contents remotely. Other options include requiring the use of "burner devices," which contain no client information on the device itself but allow for remote access through a web browser.
- *Use of personal devices.* If allowing employees to use their own devices for work purposes, implement a policy to ensure the device is secure through password protection and encryption.
- *Passwords.* Require employees to create strong passwords, which includes those that are 14 characters or longer, contain upper and lower case letters, numbers, and special characters. Also require that passwords be changed frequently, and cannot be recycled or used for multiple websites or devices. When storing passwords, consider requiring the use of a password manager program, or require storage in an encrypted document or locked cabinet.
- *Updated operating systems and software programs.* Require all employees to use updated operating systems and software programs. Also require employees to notify a manager or administrator if their system is not providing automatic updates, which usually means the program is no longer supported by the vendor and must be upgraded.

CONTINUED ON PAGE 10

- *Downloading programs.* Prohibit employees from downloading programs onto any firm device or the firm network without receiving prior authorization from a managing attorney or the IT department.
- *Clean desk.* Require employees to log out of their computer or other mobile device if leaving their desk for even a short period of time. Most devices have setting options that can be used to log a user out after a short period of time. Also require employees to clear paperwork from their desk so that client information is not exposed.
- *Opening electronic files.* Create a policy that requires electronic files received from outside sources, whether it be from a mobile storage device, file sharing program, or some other electronic source, to be opened on a standalone device that is not connected to any firm network. Or require the use of a virus scanning program.
- *Redaction and removal of metadata.* Train employees on how to redact confidential information and remove metadata.
- *Secure release of information.* Create a policy on appropriate methods for releasing information outside the firm network. For example, if providing discovery documents to opposing counsel, create a policy specifying that employees cannot mail thumb drives containing confidential client data, which are easily lost or stolen in transit. Instead consider the use of a secure file sharing program or encrypted email.
- *Internet use.* Develop specific Internet use policies. Examples include:
 - Require employees to use a secure Internet connection available only to firm members. While most WiFi connections are now password protected, some employees may work remotely, or in a building that has access to a public WiFi connection. Whichever connection is used, ensure that the connection is encrypted and a firewall is used to prevent unauthorized access.
 - Prohibit personal web browsing on firm devices.
 - Use secured websites. Only engage in online transactions if you are on a secure website, indicated by the “https” in the website address. Before entering any information, also check to be sure that the site address matches the one originally entered.
 - Require prior approval from a managing attorney or the IT department before adjusting your browser settings, such as allowing browser add-ons and plug-ins.
- *Email use.* Develop specific email use policies. Examples include:
 - Always use spam filters.
 - Beware of “red flags” in emails. Train employees to recognize red flags tied to phishing scams. For more information, go to www.osbplf.org > Blog > Evolving Scams: Don’t Let Your Guard Down.
 - Never open attachments from strangers.
 - Never open attachments sent to you unexpectedly by people you know. Malware often finds its way into an infected person’s contact list, so even if you know the person, if their system has been infected it can send a virus out to everyone in that person’s contact list.
 - Do not download any attachment sent via email, especially if the extension ends in “.exe,” which stands for “executable file” and is often used to transmit malware.

- Prior to clicking on links contained in emails, hover over the link to see if the website address is different than the link itself. Check to see if you know the sender, you were expecting receipt of the link, and that it is taking you to a secure website.
- *Working remotely.* Establish a policy that requires employees who work remotely to use a secure Internet connection, such as through a VPN, mobile WiFi, smartphone hotspot, or some other encrypted connection. Prohibit employees from connecting to the office network through a public computer or a public WiFi connection.
- *Cloud storage.* Lawyers have an ethical duty to ensure that client materials stored on a third-party server are kept reasonably secure. OSB Formal Ethics Opinion 2011-188. Don't use third-party file sharing or storage programs unless you understand the level of security and are familiar with the terms of service. Require employees to receive approval from a managing attorney or the IT department before using any cloud program for storage or sharing of electronic client materials. Or require the use of particular programs after review and approval by the managing attorney and IT department.
- *Proper deletion of data and disposal of hardware.* Create a policy regarding proper deletion of data from devices as well as disposal of hardware. For more information, see an article written by Practice Management Advisor Hong Dao, available at www.osbplf.org > Practice Management > Publications > InBrief > April 2017 > Unwanted Data: How to Properly Destroy Data in Hardware.
- *Employee departure.* Create a policy regarding employee departure, including things like return of keys or access cards, and disabling user access to the network or cloud storage programs.
- **Enforce the written security policies.** Create methods of supervision and reporting by fellow employees so that failure to follow the policies is made known to the supervisor and remedied.
- **Incident response plan.** Create an incident response plan, which is a set of protocols for managing the aftermath of a cyberattack or other type of loss, such as a lost or stolen laptop. See an article written by Practice Management Advisor Hong Dao regarding creating an incident response plan, available at www.osbplf.org > Practice Management > Publications > InBrief > October 2018 > Incident Response Plan.
- **Annual training.** Require mandatory cybersecurity training on an annual basis. Also consider periodic informal training, such as sending out emails reminding employees of potential threats and particular security policies.
- **Phishing tests to ensure compliance.** Consider hiring an IT person or company to conduct a phishing test, which simulates a cyberattack without the knowledge of employees in order to test their response.

Cybersecurity is crucial, but you don't need to have significant amounts of time or resources to implement cybersecurity training for your employees. The benefits of the time and resources invested will far outweigh the time and money spent recovering from a cyberattack.

Additional Resources

Cybersecurity employee training courses:

BrightWise (<https://www.bright-wise.com>)

Inspired eLearning
(<https://inspiredelearning.com>)

KnowBe4 (<https://www.knowbe4.com>)

Proofpoint (<https://www.wombatsecurity.com>)

Webroot (<https://www.webroot.com/us/en/business/security-awareness>)



CASES *of* NOTE

POST-CONVICTION RELIEF/STATUTE OF LIMITATIONS: In *Perez-Rodriguez v. State of Oregon*, 364 Or 489 (February 28, 2019), the Oregon Supreme Court interpreted the meaning and scope of the escape clause in ORS 138.510(3). Under the Post-Conviction Hearing Act, a petition for post-conviction relief must generally be filed within two years of a criminal defendant's conviction becoming final. That statute of limitations, however, is subject to an escape clause, allowing an untimely petition if the post-conviction court "finds grounds for relief asserted which could not reasonably have been raised" within the limitations period. In this case, the court held that, "even if a petitioner's mental illness and intellectual disability could justify applying the escape clause, petitioner's specific allegations here would not justify applying the escape clause in this case." The court reached that result based on the Legislature's intention that the escape clause should be "construed narrowly" and applied only in "extraordinary circumstances."

MEDICAL NEGLIGENCE: In *Sloan v. Providence Health System-Oregon*, 364 Or 635 (April 4, 2019), the plaintiff appealed, asserting that the trial court erred in refusing to give his requested jury instruction concerning a tortfeasor's liability for the subsequent conduct of another. The Oregon Court of Appeals agreed and reversed and remanded for a new trial. The Oregon Supreme Court affirmed, holding that, "contrary to defendant's arguments on review, (1) the court of appeals did not err in applying foreseeability principles because reasonable foreseeability limits liability in medical negligence cases; (2) plaintiff's requested jury instruction regarding an original tortfeasor's liability for the subsequent conduct of another was a correct statement of the law because an original tortfeasor is liable for the reasonably foreseeable consequences of his conduct, including reasonably foreseeable conduct and injuries by subsequent medical providers; and (3) the trial court's failure to give plaintiff's requested instruction requires reversal because the jury could have based its verdict on an incorrect understanding of the relevant law."