

## In This Issue: Information on Cybersecurity



## The Good Goodbye: Strategies for a Firm to Facilitate an Associate's Departure

*By Monica Logan*

*Editor's Note: This article is Part II of a two-part series.*

In the first installment of this series, PLF Practice Management Attorney Rachel Edwards shared tips on issues faced by departing associates. Now, we turn our attention to the firm's responsibilities and challenges when an attorney leaves.

To promote a smooth transition and protect both the firm and its clients, firms should strive to collaborate with a departing attorney. Without proper coordination, clients may experience unnecessary delays, or their case may be hastily reassigned to another firm attorney who must quickly catch up on the matter. A lack of planning and communication can lead to missed deadlines, dissatisfied clients, and attorney fee disputes. Conversely, a well-managed transition prevents issues for all involved—the firm, the departing attorney, and the client.



Professional  
Liability Fund

**inBRIEF IS PUBLISHED BY**

The Professional Liability Fund

Megan I. Livermore

*PLF Chief Executive Officer*

**EDITOR**

Tanya Hanson

*PLF Director of Communications*

*tanyah@osbplf.org*

*phone: 503.639.6911*

*toll-free: 1.800.452.1639*

[osbplf.org](http://osbplf.org)

**PROFESSIONAL LIABILITY FUND  
2025 BOARD OF DIRECTORS  
AND OFFICERS**

Michelle Johansson

Portland

*Chair*

Ali Hilsher

Eugene

*Vice Chair*

Chris Karlin

Hood River

*Secretary-Treasurer, Public Member*

John Bachofner

Camas, WA

Harshi M. Waters

Portland

Mark Johnson Roberts

Portland

Lori Kaliher

Salem

*Public Member*

Brent Smith

La Grande

Christine Coers-Mitchell

Portland

# TABLE of CONTENTS

## FEATURE

The Good Goodbye: Strategies for a Firm to Facilitate an Associate's Departure .....1

## PLF UPDATES

Claims Corner: Calling a PLF Claims Attorney .....3

Target Practice: Five Reasons Your Firm Is the Ideal Mark for a Cyber Criminal.....6

## LAW UPDATES

Approved Changes to the UTCR, Effective August 1, 2025..... 13

## LAW PRACTICE

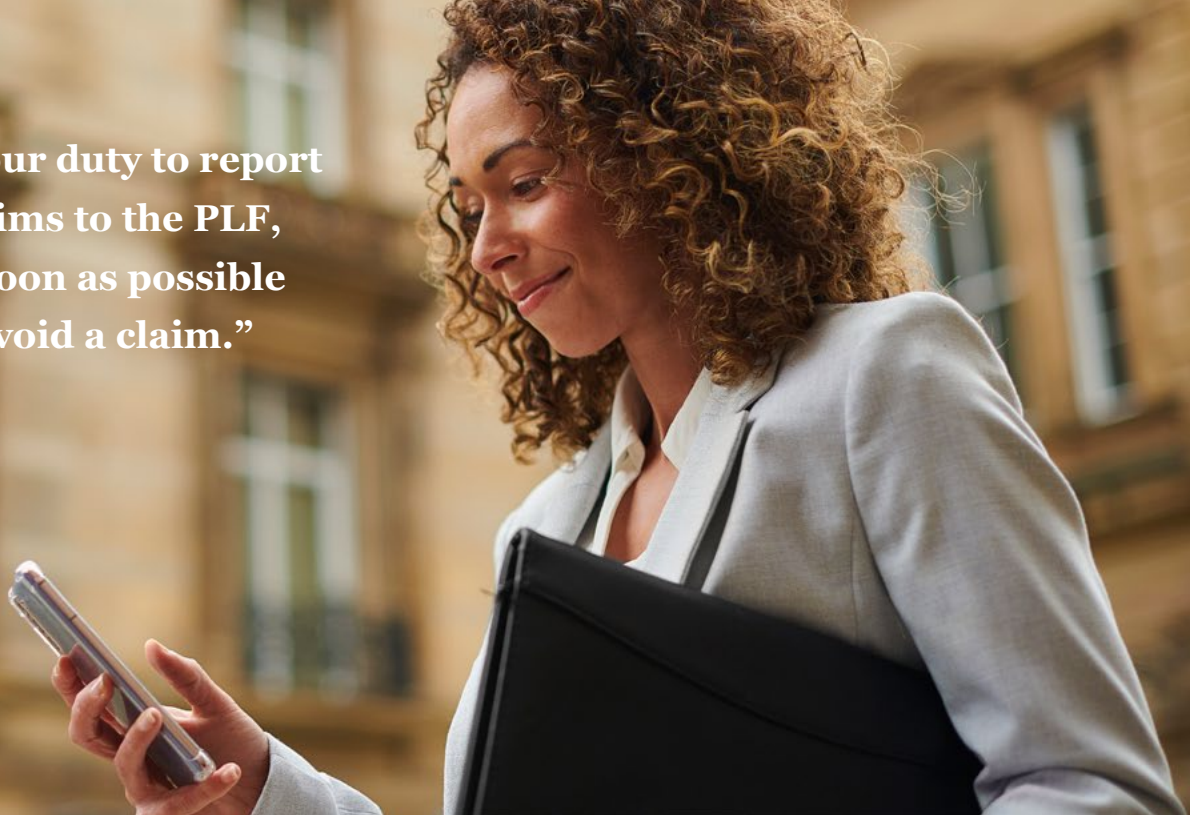
Up Against the Wire: The Growing Threat of Wire Fraud for Law Firms..... 15

Tips, Traps, and Resources ..... 20

## 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. © 2025 OSB Professional Liability Fund.

**“Aside from your duty to report potential claims to the PLF, doing so as soon as possible may help avoid a claim.”**



## Claims Corner – Calling a PLF Claims Attorney

---

*By Heather Bowman*

PLF claims attorneys are available to help covered parties deal with claims situations. Every business day, claims attorneys answer calls from Oregon legal practitioners in all practice areas to help address and avoid claims. Read on for tips to maximize this valuable resource.

### Reasons to Call a Claims Attorney

#### **1. SOMEONE HAS MADE A CLAIM AGAINST YOU**

The most obvious reasons to call the PLF are because you were served with a legal malpractice lawsuit alleging claims against you, you have learned that such a lawsuit has been filed against you, or someone has notified you that they are making a claim against you. If you have already been sued for an alleged error in representing a client or you learn that a lawsuit has been filed alleging claims against you, call the PLF right away. Have a copy of the lawsuit handy so you

can identify the parties and the case number. If the claim is a covered claim, the PLF will hire counsel to defend you in the action.

You should also call the PLF immediately if you are contacted by someone alleging a claim against you based on an alleged error in representing a client. Sometimes such claims are presented to the covered party by a current or former client or by an attorney representing the current or former client. These claims are sometimes accompanied by a demand for compensation or for curative or repair action. If you receive notice of such a claim in writing, have the

written demand available when you call the PLF so you can forward it to the claims attorney who is addressing your call.

You can also report a claim through the PLF website at [osbplf.org/claims/reporting-a-claim.html](https://osbplf.org/claims/reporting-a-claim.html). After you report online, you will be contacted by a claims attorney.

## **2. YOU WERE SERVED WITH A SUBPOENA FOR YOUR CLIENT FILE OR DEPOSITION TESTIMONY**

If you were served with a subpoena, or you are contacted by a third party for information about representation of a client or former client, contact the PLF before providing any materials or agreeing to testify. Similarly, if you receive a request for information in a post-conviction relief matter, even if the request is made by your former client, we recommend that you contact the PLF. The PLF has discretionary authority to retain counsel to represent covered parties in discovery matters, including requests for deposition, trial testimony, or file materials. The PLF may retain counsel to help you navigate issues such as client confidentiality and privilege, which may help avoid larger problems.

For more detailed information on responding to a client information subpoena, see “Bar Counsel: Client Information Subpoenas: OSB & PLF Guidance for Responding, Protecting Client Confidences,” *OSB Bulletin*, January 2025.

## **3. YOU MADE AN ERROR REPRESENTING A CLIENT**

Under the PLF Primary Coverage Plan, you have a duty to report if you become aware of facts or circumstances that reasonably could be expected to be the basis of a claim. The Plan requires that you provide written notice to the PLF as soon as practicable of the specific act, error, or omission; any damages or injury that have resulted or may result; and the circumstances under which you first became aware of the act, error, or omission. See 2025 PLF Primary Coverage Plan VIII.B (available on the PLF website at [osbplf.org/coverage/what-is-my-coverage.html](https://osbplf.org/coverage/what-is-my-coverage.html))

Aside from your duty to report potential claims to the PLF, doing so as soon as possible may help avoid a claim. Sometimes the PLF is able to engage in a repair to get the case back on track. Other times, a PLF claims attorney may be able to advise you about steps that might avoid a basis for a claim or mitigate the client’s loss. Repairs are discretionary and depend on a variety of factors, but no repair is possible if you fail to report the issue.

If you made an error that you are thinking about fixing on your own, call the PLF first. Self-repair may be the best approach if your client provides informed consent, but you must still report the claim. Additionally, the PLF claims attorney will likely assist you in addressing any obligations to disclose certain information to a client about the situation.

## **4. YOU ARE ACCUSED OF MAKING AN ERROR**

If your client or opposing counsel accused you of making an error, or if you think you might have made an error but are uncertain, contact the PLF. Even if no claim has been made, you have a duty to report the potential claim to the PLF.

## **5. YOU HAVE QUESTIONS**

PLF claims attorneys receive many calls from legal practitioners who have questions about substantive or procedural legal issues. They are always willing to discuss a situation with you or brainstorm ideas, but the opinion of a claims attorney holds no sway with the courts and they cannot perform legal research for covered parties. If you find yourself in unfamiliar legal territory, you may wish to associate co-counsel experienced in that area of law.

Claims attorneys also receive calls from practitioners who are dealing with challenging clients. They cannot intervene in your attorney-client relationship but can discuss ideas for working through your issues, or, if necessary, strategies for terminating your attorney-client relationship to minimize exposure of a malpractice claim.



PLF claims attorneys also receive calls seeking ethics advice. While malpractice and ethics can be closely intertwined, your call to a PLF claims attorney should be related to a claim of malpractice or an attempt to avoid malpractice. If you are seeking free ethics advice, you should call the OSB Ethics Helpline at 503.431.6475. If you require confidential ethics advice, you should retain private counsel.

## Preparing for Your Call

If you have previously worked with a claims attorney or know who you want to work with, you are welcome to call that person directly. Alternatively, you can call the PLF's receptionist, who will direct your call to one of the claims attorneys handling informational calls that day.

Your communications with the PLF about claims or potential claims are privileged as long as you protect that privilege, so be sure to call from a private location. You may wish to have other involved attorneys on the call with you, but do not include your client in the call. Make sure you are somewhere you will be able to provide details about the issue and answer questions.

Be sure to have all relevant information available, including the names of the parties and counsel,

the case number for a matter in litigation, and all relevant dates.

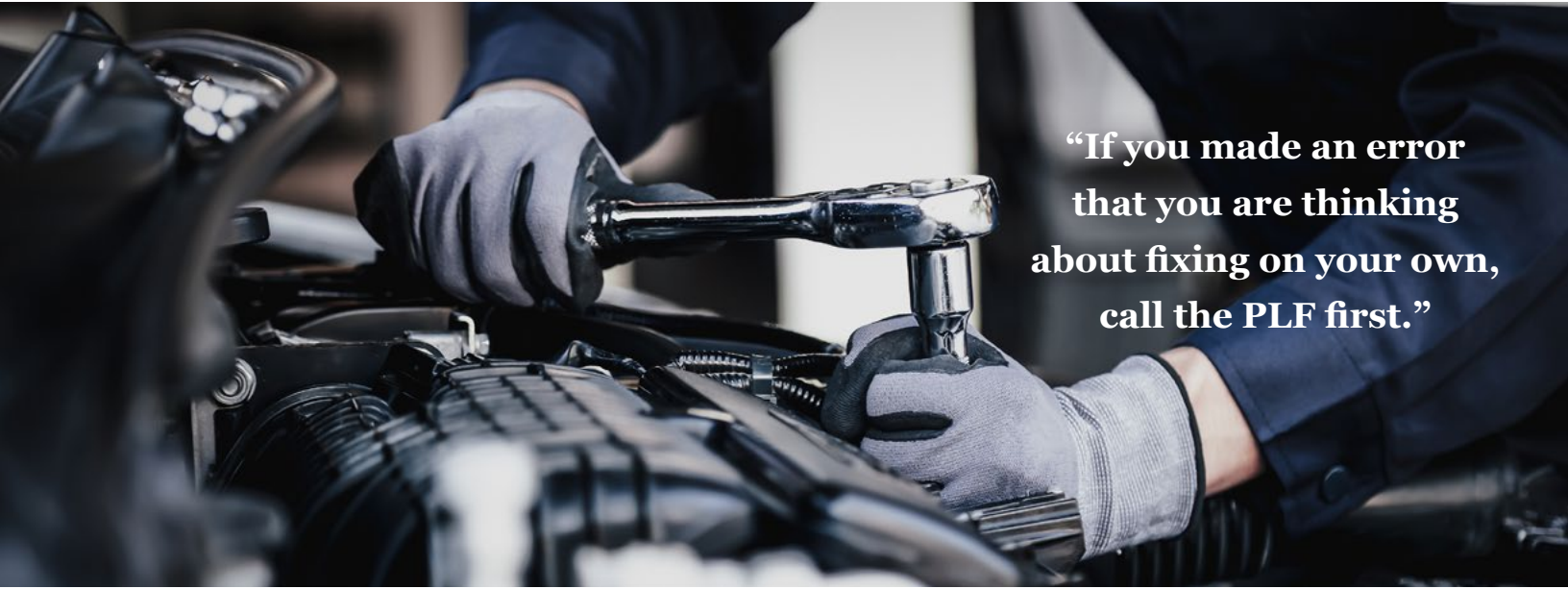
PLF claims attorneys are here to help covered parties respond to and avoid malpractice claims. Give them a call at 503.639.6911! ■



Heather Bowman is the  
PLF General Counsel.

### OTHER WORKS BY HEATHER BOWMAN

- “Counsel Column – Extended Reporting Coverage: Am I Covered Against Malpractice Claims After I Retire or Leave Private Practice?” *inBrief*, Issue 146, December 2024
- “Counsel Column – Thank You for Your Service: Malpractice Coverage for Pro Bono Work,” *inBrief*, Issue 145, May 2024
- “Claims Corner – Calling a Claims Attorney,” *inBrief*, Issue 141, October 2020



**“If you made an error  
that you are thinking  
about fixing on your own,  
call the PLF first.”**



“Essentially, law offices must be concerned not only with their internal security practices but also the security systems of their vendors, clients, and other contacts.”

## Target Practice: Five Reasons Your Firm Is the Ideal Mark for a Cyber Criminal

---

*By Melanie Hughes*

Cyber crimes against lawyers are on the rise. A 2023 ABA survey revealed that an astounding 29% of law firms have experienced a data breach, and this number is growing. Also in 2023, a cyber threat intelligence company, Checkpoint Research, reported that **1 out of every 40 cyber incidents was perpetrated against a law firm.**<sup>1</sup> How does this happen? Why are practicing attorneys such appealing marks?

Law firms make attractive targets to cyber criminals for a variety of reasons:

### 1. THEY POSSESS VALUABLE DATA

This includes PII (personally identifiable information), financial account information, tax filings, settlement and/or nondisclosure agreements, and in some cases intellectual property such as trade secrets, patents, and copyrights. This data can then be used or sold to commit crimes like fraud, identity theft, and extortion.

### 2. THEY MAY LACK RESOURCES TO KEEP UP WITH EMERGING TECHNOLOGY

While larger law offices may have more data, smaller practices make ideal “soft targets” because they often lack the financial resources to continuously update their systems in the face of new threats. Their staff might also lack sufficient training to identify social engineering



attempts like fraudulent instruction or phishing. A 2024 report by CISA (Cybersecurity & Infrastructure Security Agency) confirms this trend, citing that less than 50% of law firms offer training in cybersecurity to their staff.<sup>2</sup> Threat actors often prey on smaller outfits because they possess valuable data with fewer obstacles in place to protect it.

### 3. THEY RISK REPUTATIONAL HARM

Cyber breaches rarely stay private. Instead, they often require notices to affected parties and government entities. The belief or perception that a firm is unable to secure client information may lead to reputational harm, and hackers know that partners will consider meeting their demands to preserve their professional reputation. Experts caution, however, against paying threat actors or meeting their demands, as this encourages and funds future criminal activity. If the malicious actor is a sanctioned person or entity according to the U.S. State Department, it may also be illegal to pay them. For this reason, contacting law enforcement is a crucial first step.

## Important Calls to Make

Firms with PLF Excess Coverage should call 503.639.6911 during regular business hours. Firms without PLF Excess should contact all insurance carriers to provide notice of the incident. Even those without specialized cyber or crime coverage policies might find this productive, as commercial policies can carry extensions or endorsements that provide limited coverage for electronic data-related claims.

Contact the PLF before paying any type of demand, no matter how minimal. Firms without PLF Excess can obtain guidance and resources through the PLF Practice Management Assistance Program (same telephone number).

### 4. THEY HAVE CLIENTS WHO CAN BE EASILY EXTORTED

While the law entity is often the primary goal, clients can also be extorted to keep their personal or business information private. Hackers will often threaten to contact clients if the demand is not paid, which could lead to liability claims for failing to protect client information. Unsurprisingly, paying their demand is no guarantee that the malicious actors will refrain from extorting the clients.

### 5. THEY PROVIDE A GATEWAY TO OTHER VULNERABLE SYSTEMS

Lawyers tend to have large social networks. They interact with individuals, businesses, financial institutions, and government/municipal entities, as well as lawyers in other law firms. Legal practices are prime targets because a threat actor might meet less resistance accessing those other entities' systems through deceptive practices like phishing, "spoofed" emails, or exploitation of backdoor vulnerabilities. According to a Verizon Data Breach Investigations Report, over 80% of data breaches stem from phishing.<sup>3</sup>

Law firm partners should assume that any data they collect or possess can be stolen through vulnerabilities in a third-party's system. Cybersecurity Dive quotes a 2023 report from Security Scorecard and the Cyentia Institute revealing that "98% of organizations worldwide have integrations with at least one third-party vendor that has been breached in the last two years."<sup>4</sup> The same Cybersecurity Dive article cites a report from Black Kite, a cyber security risk platform, that credits **63 vendor** breaches as the catalyst for cyber intrusions at almost **300 companies**. According to Bob Maley, Black Kite CSO, "while the exact method of access is not usually disclosed or immediately known, unauthorized network access often is due to phishing, stolen credentials, or vulnerabilities in access control."<sup>5</sup> Essentially, law offices must be concerned not only with their internal security practices but also the security systems of their vendors, clients, and other contacts.

To address the risk arising from outside networks, practitioners should consider conducting a Vendor

Risk Assessment for all outside parties with whom the partners or staff share data or regularly interact. Questionnaires probing a vendor's authentication and access controls—use of multi-factor authentication, firewalls, anti-virus/anti-malware software, and end-point monitoring—are important. Having an Information Security Policy, engaging in staff training, conducting routine system vulnerability testing, and performing off-site backups of data are also critical.<sup>6</sup>

## Mitigate Your Chances of Becoming a Cyber Victim

Data is valuable to hackers, so one way to mitigate the potential impact of a cyber breach is by evaluating the data the law firm collects and stores several times throughout the year. Evaluate your answers to the following questions:

### WHY DO WE COLLECT THE DATA WE COLLECT?

- Is the data necessary to perform essential business functions?
- Does the risk of collecting/storing/using the data outweigh the risk of the data being accessed or stolen by malicious actors?

### WHO HAS ACCESS TO THE DATA?

- Are we sharing sensitive data with external vendors or other third-party entities?
- Do these other parties need this sensitive data to complete their prescribed tasks?
- Is the current method of transferring/sharing the data the ONLY way to provide essential information to a third-party? (Consider telephone and secure email protocols as alternative methods.)

### WHEN SHOULD WE DISPOSE OF DATA?

- Do we have a data purge policy?
- What are the legal or regulatory requirements for holding physical and/or electronic data?
- Does the benefit of storing this data longer than legally required outweigh the risk of the data being accessed or stolen by malicious actors?

Despite an awareness of the risks and heightened security measures, cyber incidents still occur. For this reason, law partners should carefully consider the level of risk they are willing to assume following a cyber breach and whether commercial cyber and/or crime insurance is a prudent expenditure. Cyber and crime policies vary greatly among carriers, so it is important to review coverages and exclusions carefully before purchasing.

Legal practitioners interested in cyber insurance may wish to consider PLF Excess Coverage. While cyber-related claims are excluded under the PLF Primary Plan, PLF Excess Coverage *includes* cyber coverage of \$100,000 for firms with 1-10 attorneys and \$250,000 for firms with 11 or more attorneys. Higher-limit cyber coverage may also be available for purchase on an underwritten basis. The 2025 Cyber Liability and Breach Response Endorsement is available at [osbplf.org/excess/cyber-coverage.html](https://osbplf.org/excess/cyber-coverage.html).

Applications for PLF Excess Coverage are accepted throughout the year. Visit [osbplf.org](https://osbplf.org) for more information or to apply for coverage.

Questions about Excess Coverage?

Email [excess@osbplf.org](mailto:excess@osbplf.org). ■



**“A 2023 ABA survey revealed that an astounding 29% of law firms have experienced a data breach, and this number is growing.”**



## ENDNOTES

1 “Cybersecurity Checklist for Vendor Management—Vendor Security,” Burr & Forman Security, February 15, 2023, <https://www.burr.com/newsroom/articles/Cybersecurity-Checklist-Vendor-Management-Vendor-Security>

2 “Law Firms Face Rising Cyber Threats: Are They Ready?,” GCS Network, November 4, 2024, <https://globalcybersecuritynetwork.com/blog/law-firms-cyber-threats-readiness/>

3 “Top Cybersecurity Survival Guides for Small Businesses in 2025,” GCS Network, November 1, 2023, <https://globalcybersecuritynetwork.com/blog/top-cybersecurity-survival-guides-for-small-businesses/>

4 David Jones, “Dive Brief: 98% of organizations worldwide connected to breached third-party vendors,” Cybersecurity Dive, February 2, 2023, <https://www.cybersecuritydive.com/news/connected-breached-third-party/641857/>

5 Jones, “Dive Brief: 98% of organizations”

6 “Cybersecurity Checklist for Vendor Management—Vendor Security,” Burr & Forman Security, February 15, 2023, <https://www.burr.com/newsroom/articles/Cybersecurity-Checklist-Vendor-Management-Vendor-Security>



Melanie Hughes is the PLF Professional Liability Underwriter.

## OTHER WORKS BY MELANIE HUGHES

- “Don’t Get Caught with Your Plans Down: What Is a Retroactive Date and Why Does It Matter?” *inBrief*, Issue 146, December 2024
- “Bundle Up This Winter With Excess Coverage Through the PLF,” *inBrief*, Issue 144, December 2023
- “Excess Coverage: The Contract Attorney Conundrum,” *inBrief*, Issue 143, August 2023

**THERE’S ENOUGH TO  
WORRY ABOUT. DON’T  
LET COVERAGE KEEP  
YOU UP AT NIGHT.**



Excess  
Coverage

Apply: [osbplf.org/excess](https://osbplf.org/excess)  
Info: 503.639.6911

## Associate Attorney Anne's Departure Journey

Let's return to our story about Associate Anne, a fifth-year attorney leaving to start her own practice. She specializes in estate planning and trust litigation and is currently handling a case set for trial in just two weeks. After notifying the firm, Anne will discuss the status of the upcoming trial with the firm to determine who will take over the matter before her departure.

The firm's managing partner, Mike Stickler, does his best to adhere to all ethical obligations. His practice focuses on family law and estate planning, along with a few trust litigation cases. The firm also has one other staff attorney, Ike, who exclusively handles estate planning matters.

## Timing of Departure and Firm's Reaction

The timing of an associate's departure can significantly impact client interests. For example, if there is not enough time for the firm attorneys to familiarize themselves with a case, they may not be adequately prepared to represent the client at trial. Sometimes, an associate may depart suddenly, or a firm may unexpectedly terminate their employment. In such cases, the firm may need to revoke the departing attorney's access to files and other systems abruptly. When an associate leaves immediately after notice or termination, the firm is responsible for notifying their clients and reassigning their cases. A notification template can help streamline this process. (An example notification letter is available in the PLF Practice Aids, under the category "Joining or Departing a Firm.") Unplanned exits can upset client relationships, create misunderstandings, and lead to problems with the representation.

To minimize issues, it's best to avoid sudden departures whenever possible. Establishing a structured transition plan will aid the orderly transfer of cases. Open communication between the associate and firm is key—discussing case statuses and informing the other party of any notices received. In determining whether to offer

continued representation to the departing associate's clients, the firm needs to consider upcoming deadlines, current attorney workloads, and requisite practice area experience. Most importantly, both the firm and the associate must prioritize handling the client's matter appropriately at every stage of the transition.

In our example with Associate Anne, she and Mike review her case list and assess urgent deadlines. Before deciding whether to take over any of Anne's cases, Mike and Ike evaluate whether they have the necessary experience and capacity to manage the cases effectively. After their review, they conclude Ike can handle Anne's simple estate planning matters, but her trust litigation cases would be too complex and demanding for the firm.


In the urgent trust litigation matter, the time is too short for Mike to get up to speed without risking harm to the client's case. To ensure proper handling and avoid potential delays, Mike asks Anne to complete the trial before her official departure.

## Client Notifications

The client notification process is crucial, because Oregon Rules of Professional Conduct 1.2 and 1.4 establish that clients have the right to determine the goals of their representation, including who represents them. Before deciding, clients must be fully informed of their options.

Notification can occur in one of two ways: either the firm and the departing attorney send a joint letter, or each party sends a separate letter. A joint letter is ideal when both the firm and the attorney agree on the options offered to the clients. If there is a disagreement about the letter or the clients' options, however, firms and associates may choose to send separate letters.

In Anne's case, she and the firm agree that estate planning clients can choose to remain with the firm, transition to Anne's practice, or find a different firm to represent them. They decide to send a joint letter outlining those options and include Anne's email address for clients who wish to contact her directly. If either Anne or the firm lack capacity to manage certain cases, they can modify the letter to omit that option.



**“As much as possible, firms would be well-served to proactively coordinate with the departing associate to minimize potential disruptions and uphold their ethical responsibilities.”**

For instance, the letter to the trust litigation clients does not offer continued firm representation. Before sending any letters, Mike should allow Anne to review them for accuracy.

For clients choosing to leave, the firm will want to start preparing to transfer those cases by reconciling trust balances and gathering the relevant case files.

## Notice of Substitution or Withdrawal

During this transition period, clear communication is critical to effectively preserve client interests. Both the departing associate and the firm share a responsibility to prevent any negative impact on client matters. Thus, they may need to work together to manage upcoming deadlines or court appearances. According to Oregon State Bar Formal Ethics Opinion 2005-70, comment three, neither the firm nor the lawyer should deny access to client or matter-related information necessary to protect a client's interests. This guidance aligns with ORPC 1.1, which addresses competency in handling a client matter, and ORPC 1.3, which requires a lawyer's diligence in representation. Once the associate or the firm receives a client response, they must promptly share that information with the other party.

Finally, the departing associate is responsible for formally withdrawing as attorney of record. However, if another firm attorney is taking over, the new attorney should file a substitution of attorney immediately. Any delay could cause court notifications to be sent

to the wrong attorney, potentially resulting in missed deadlines or other issues.

## Managing Client Choices and Transferring Files

As clients respond, the firm should transfer files promptly, prioritizing urgent matters. Maintaining a complete list of Anne's cases and using it to track client decisions and file transfers will help facilitate a smooth transfer process. File transfers can be labor-intensive and time-consuming if documents are not consolidated in a single storage location. Nonetheless, the firm ought to make every effort to quickly gather and send all client files to the appropriate recipients, whether the client or the associate's new firm.

As part of the departure process, the firm must provide the associate with a conflict list, including key details about the parties and the matter so the associate can perform conflict checks in the future. Sometimes the associate may request additional information, such as client phone numbers or addresses. While firms may hesitate to provide this information out of concern that the associate could later solicit clients, it's more important to focus on providing the information necessary for a proper conflict search. For instance, cases involving real estate may require a client's address to conduct an adequate conflict check. Ultimately, it is the firm's decision whether to share client contact details. When the firm provides the necessary conflict details and the departing attorney honors the firm's



guidelines regarding client information, both parties foster a smooth and respectful transition.

If any return of client funds is necessary, Anne may need to request an off-cycle trust account reconciliation and refund. If she continues to encounter delays, she should politely email or call the appropriate contact person at the firm to follow up. Remember, she cannot remove firm property without the firm's consent, which includes client contact information, client files, and forms—even forms she may have drafted before or during her time with the firm.

## Other Potential Issue: Fees

Another potential issue is outstanding fees, particularly when a client has an overdue invoice or fees are paid during the final stages of the matter. If a client follows the departing attorney, they might not know how to settle any remaining balance with the original firm. To prevent misunderstandings, the firm would be wise to communicate with the client about the amount owed and accepted payment methods as part of their disengagement process. If a dispute arises between the firm and the departing associate over fee allocation, they should seek to resolve it professionally and in line with any applicable agreements or ethical standards. Ideally, they can settle any fee-related issue in a manner that prioritizes the client's best interest and the exciting opportunities that lie ahead.

## Conclusion

By maintaining collaborative communication and carefully planning the transition process, firms and attorneys can support a seamless change that protects client interests. As much as possible, firms would be well-served to proactively coordinate with the departing associate to minimize potential disruptions and uphold their ethical responsibilities.

While ethics rules and Oregon State Bar Formal Ethics Opinions provide guidance, they may not address every scenario that arises during a transition. In the absence of clear direction, both the associate and firm must do their best to collaborate to serve the client.

For specific questions, firms can consult with a practice management attorney or seek ethical guidance from the Oregon State Bar Ethics Helpline at 503.431.6475. ■



Monica Logan is a PLF Practice Management Attorney.

### OTHER WORKS BY MONICA LOGAN

- “Client Onboarding Matters: Three Tips for a Smooth Journey,” *inPractice* blog post, July 24, 2025
- “Blueprint for a Successful Firm: The Business Plan,” *inPractice* blog post, March 10, 2025
- “*inBrief* Roundup: Top Three Practice Management Articles,” *inBrief*, Issue 143, August 2023

## PLF Resources for Departing Associates

The PLF has several practice aids with helpful information for the departure process. Visit [osbplf.org](https://osbplf.org) > Services > CLEs & Resources > Practice Aids > Transitions and Closing a Law Practice > Joining or Departing a Firm. Resources include:

- Checklist for Departing Lawyers
- Departing a Firm Letters
- Authorization for Transfer of Client File When Attorney Departs Firm
- Email Communications for Departing Lawyers

Also see PLF CLE “On the Move: Navigating Employment Transitions in the Legal Profession,” presented June 11, 2025.

## Approved Changes to the UTCR Effective August 1, 2025

**Chief Justice Flynn has signed Chief Justice Order (CJO) 25-012, which approved changes to the Uniform Trial Court Rules (UTCR), effective August 1, 2025.**

**5.010 – CONFERRING ON MOTIONS UNDER ORCP 21, 23, AND 36–46** Amended the rule to add a conferral requirement for disputes relating to ORCP 55 (subpoenas).

**5.100 – SUBMISSION OF PROPOSED ORDERS OR JUDGMENTS** Amended the rule to require certification of the advance service date, added a new exemption regarding waivers of appearance, and made conforming amendments to the certificate of readiness.

**5.180 – CONSUMER DEBT COLLECTION** Amended to simplify the rule language and clarify requirements regarding the consumer debt collection disclosure statement.

**6.080 – MARKING EXHIBITS** Amended subsection (3) to require a list of premarked exhibits to be submitted to the court as ordered by the assigned judge to align with the time for submitting exhibits under UTCR 6.050(3).

**8.010 – ACTIONS FOR DISSOLUTION OF MARRIAGE, SEPARATE MAINTENANCE AND ANNULMENT, AND CHILD SUPPORT** Amended UTCR 8.010(4) to simplify the terminology used regarding required “attachments” to a Uniform Support Declaration (USD) and USD related “schedules and attachments required by the schedules.”

**9.010 – MAILING PROBATE MATERIALS TO THE COURT** Repealed the rule regarding the mailing of probate documents to the court.

**9.020 – APPROVAL OF BONDS** Amended to require that bond change requests be made by motion or by request in an annual accounting to conform with local court practices.

**9.040 – SETTLEMENT OF PERSONAL INJURY CLAIMS IN PROBATE CASES**

Amended to require probate court approval of settlements of personal injury claims on behalf of protected persons.

**9.050 – RESTRICTED ACCOUNTS** Amended to require that a depository's signed writing include a statement acknowledging the consequences of unauthorized withdrawals.

**9.060 – FEES IN ESTATES, GUARDIANSHIPS AND CONSERVATORSHIPS** Amended to require that affidavits supporting a request for attorney fees also include a fee itemization in the manner provided in UTCR 5.080.

**9.160 – FORM OF ACCOUNTINGS** Amended to add prefatory language addressing important components of required accountings and to add a new section to create a beginning total balance requirement to the form of accountings.

**9.170 – FIDUCIARY DISCLOSURE IN ACCOUNTINGS** Amended to add a new disclosure requirement regarding advancements and reimbursements made to fiduciaries.

**9.180 – VOUCHERS AND DEPOSITORY STATEMENTS** Amended to allow fiduciaries to file vouchers and depository statements as confidential documents under a separately captioned court filing.

**9.200 – AUDIT OF ACCOUNTING AND RELATED DOCUMENTS** Adopted a new rule governing a court's authority to audit case filings regarding a fiduciary's administration of estates, guardianships, and conservatorships.

**9.300 – APPOINTMENT OF GUARDIANS IN ADOPTIONS** Amended to clarify language regarding appointment procedures.

**9.330 – GUARDIAN'S REPORT IN MINOR GUARDIANSHIPS** Adopted a new rule requiring the appointed guardian of a minor to file an annual written report with the court.

**9.400 – APPOINTMENT OF COURT VISITOR** Adopted a new rule in place of the existing UTCR 9.400 (previous UTCR 9.400 – Court Visitor's Report now renumbered as 9.420) to create a standard process to appoint court visitors.

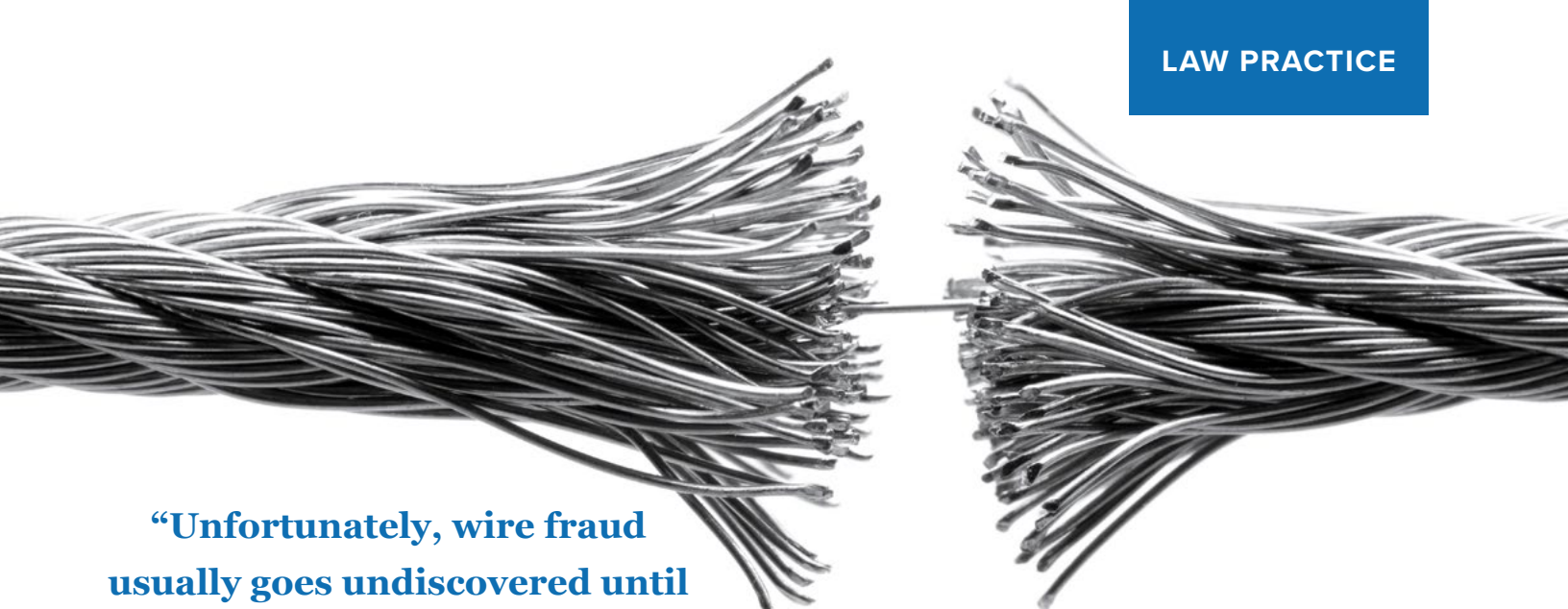
**9.420 – COURT VISITOR'S REPORT** Renumbered from UTCR 9.400 to 9.420 and amended to mandate that a visitor's report is a confidential filing and to identify persons who must receive a copy of the report.

The approved changes are available online at [www.courts.oregon.gov/utcr](http://www.courts.oregon.gov/utcr). The Preface to the 2025 UTCR includes detailed explanations of the changes.

The UTCR Committee's next meeting is October 24, 2025. The committee welcomes proposals for changes to the trial court rules. Submit proposals by August 31, 2025, to [utcr@ojd.state.or.us](mailto:utcr@ojd.state.or.us), or mail them to UTCR Reporter, Office of the State Court Administrator, Supreme Court Building, 1163 State Street, Salem, OR 97301-2563.







**“Unfortunately, wire fraud usually goes undiscovered until it is too late for recovery.”**

## Up Against the Wire: The Growing Threat of Wire Fraud for Law Firms

---

*By Rachel Edwards*

Imagine this scenario: You represent a company in a months-long negotiation and finally settle the dispute in favor of your client for a large six-figure sum. After a few back-and-forth emails, you verify with your client the settlement agreement terms, and they provide you instructions on where to wire the funds. Soon after you wire the money, your client calls you asking why they haven’t received the money yet. A sinking feeling in your stomach tells you that something has gone wrong. You call the bank immediately and realize your client’s email was hacked, and the money was sent to the hacker’s bank account instead. Because the funds have already been transferred, nothing can be done to reverse the transaction.

This isn’t just a cautionary tale—it’s a chilling reality. A firm in Portland was recently the victim of wire fraud. Although the Portland firm was able to reverse the transaction due to unique and rare circumstances, another firm in Oregon was not so lucky. One of the

Portland firm’s partners—let’s call him George—has agreed to share his story in hopes of shedding light on this rapidly growing and dangerous type of fraud, helping fellow lawyers recognize and guard against it.

## George's Story

### LARGE SETTLEMENT

George's firm represented a business in a property dispute matter. The firm settled the dispute on behalf of their client and began the process of facilitating the transmission of a large settlement amount from the opposing party to their client.

### EMAIL COMPROMISE

At the time of the settlement, the client's email had already been hacked, and it is suspected the hackers had been monitoring and manipulating the client's email account for some time. The hackers had even set up automatic rules in the client's email program so that selected emails from George's firm went directly into a private folder hidden from the client. The hackers were now aware of the pending receipt of

settlement money and ready to insert themselves into email communications when time came for payment.

### WIRE FRAUD

George emailed the settlement agreement to his client and said in the body of the email that he would be calling the client to confirm understanding of the terms. Knowing George would be calling the client, the hackers allowed this email to be seen by the client. George called the client, and they signed the settlement agreement and emailed it back to George. George also sent the client an email requesting wiring instructions. The hackers intercepted and returned fraudulent wiring instructions using the client's email address. Assuming the wiring instructions were coming from the client, George transmitted that information to opposing counsel. Unfortunately, no action was taken to verify the wiring instructions with the client, and the opposing party wired the money

## Just Launched! Free Trust Accounting & Billing Software for OSB Licensees

As an Oregon State Bar licensee, you get access to Smokeball Bill completely free. This trust accounting and billing software is valued at \$588 per user/per year but is now accessible at no cost to all Oregon State Bar licensees.

Smokeball Bill helps law firms with:

- Easy trust account management
- Flexible invoicing options
- Fast and simple time tracking

Sign up today at [www.smokeball.com/oregonbill](http://www.smokeball.com/oregonbill)



to the hacker's bank account. The hacker then tried to immediately transfer the money to a foreign bank but made an error, resulting in a delay of the transfer. The delay allowed George's firm to contact the banks involved, freeze the funds, and reverse the initial wire transfer. The funds were returned to the opposing party, who proceeded with a proper wire transfer to George's client.

Here, thankfully the delay allowed George's firm time and opportunity to freeze funds and reverse the transaction. Unfortunately, wire fraud usually goes undiscovered until it is too late for recovery. Fraudsters wear many different hats, making it very difficult to prevent wire fraud. In addition to posing as the client, fraudsters may pretend to be a lawyer or staff person in the firm, or a financial institution or other third party related to the transaction. While email or system infiltration is a common tactic, they may also use spoofed email addresses and phishing links (explained further in this article).

## Increase in Wire Fraud

According to the Federal Trade Commission,<sup>1</sup> consumers reported losing more than \$10 billion to fraud in 2023, marking a 14% increase over reported losses in 2022. Wire transfers are a form of electronic payment that sends money directly from one bank account to another, making the funds typically available in the recipient's bank account the next business day or even the same day. The recipient's desire for the quick receipt of money, increased remote interactions since COVID, and a decline in use of paper checks combine to make wire transfers a popular method of payment.

## Coverage

Wire fraud is not covered under the PLF Primary Plan or most commercial property or general liability policies. Even if you have cyber insurance through PLF Excess Coverage or another commercial insurance carrier, it is possible that wire fraud will

not trigger coverage due to conditions and exclusions in the policy. Before purchasing cyber or crime insurance, it is critical that you carefully read through and understand the coverage offered. The best way to avoid wire fraud is to be proactive. Think of insurance as the last tool in your cybersecurity toolbox. While insurance can possibly offer a safety net, it is also possible that the circumstances of the incident could fall outside coverage. Contact our Excess Department at [excess@osbplf.org](mailto:excess@osbplf.org) if you have questions about wire fraud coverage. Take the following steps to lessen your chances of becoming a wire fraud victim.

## Tips to Prevent Wire Fraud

### 1. MAINTAIN TRUSTED CONTACT INFORMATION

When opening a new matter, gather trusted contact information for your client(s) and all parties involved at the outset of representation. Also be vigilant about verifying known, trusted representatives of the recipient, if any.

### 2. GUARD AGAINST EMAIL COMPROMISE

Email is vulnerable to attacks and is often used as a vehicle to commit wire fraud. Take these steps to prevent email compromise:

1. **Use encrypted email or a client portal to exchange sensitive information.** Don't use a free email program. Use a paid, business version. If you have Microsoft 365 Business Premium and use the hosted Exchange server, you have built-in encryption. Other options include email encryption add-on programs, such as Trustifi (<https://trustifi.com/>) or TitanFile (<https://www.titanfile.com/>). A client portal is an encrypted communication and document sharing platform. Many practice management software programs, such as Clio (<https://www.clio.com/>) and MyCase (<https://www.mycase.com/>), include this feature.

<sup>1</sup> <https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public>



## 2. Use spam filters and check email

**addresses for slight changes.** Install a spam filter to help identify emails containing malicious content. Check email addresses because cyber criminals may create a spoofed email address that is very similar to the real sender's address (e.g., [smithlaw@outlook.com](mailto:smithlaw@outlook.com) vs. [smithlaw@outloook.com](mailto:smithlaw@outloook.com)).

## 3. Enable multifactor authentication

**(MFA) for all email accounts.** Require an additional method of authentication, such as a secure code sent to a secondary device, in addition to a password.

## 4. Recognize phishing emails.

Don't open attachments in emails from strangers or even unexpected attachments from those you know. Contact the person by phone using a verified number. Don't click on links in emails, as they may redirect you to an illegitimate website.

## 3. SECURE YOUR FIRM'S NETWORK

While you cannot control the network vulnerabilities of outside parties, you can minimize your firm's own vulnerabilities by maintaining updated technology, securing your internet connection, and using strong, regularly updated passwords. See our practice aid for more information about cybersecurity at <https://www.osbplf.org/services/resources/> > Practice Aids > Technology and Data Management > Security and Data Breach > Checklist to Prevent and Prepare for a Data Breach. Require mandatory cybersecurity training for all attorneys and staff at least annually. Consider training courses through companies such as KnowBe4 (<https://www.knowbe4.com/>), or Proofpoint (<https://www.proofpoint.com/us/products/mitigate-human-risk>).

## 4. VERIFY WIRING INSTRUCTIONS USING MFA

Add another layer of protection through MFA by confirming the wiring instructions using a different medium than the initial message. Because the sender's email or network may already have been hacked, you do not want to rely on a single source of information. For instance, after receiving an email with wiring

instructions, call the sender using a trusted phone number, such as the one from the intake sheet or a reliable directory. Do this *even if you receive instructions from someone inside your organization*. In-person verification is also a valuable option when feasible. DO NOT rely solely on a phone number provided in one type of communication.

## 5. REQUIRE ADDITIONAL IDENTIFYING INFORMATION

Also require the provider of wiring instructions to verify their identity with a pre-established code word kept offline. For example, ask the person sending instructions to provide you with the code before verifying wiring instructions by phone. The same direction applies to a videoconference or in-person meeting—require the person to provide the code and ask them to show a valid identification card, like a driver's license.

## 6. RECOGNIZE RED FLAGS

Common red flags include receipt of instructions from a different email address than the one gathered at the outset of representation, requests for funds to be sent to accounts not in the recipient's name, changes to wire instructions, or a request that money be sent to a location outside the recipient's jurisdiction. Train employees to question anything suspicious, stop the process, and immediately report concerns to a managing partner.

## 7. CREATE A DETAILED FUNDS TRANSFER INSTRUCTIONS VERIFICATION CHECKLIST

This checklist is a culmination of all the above safety protocols. See our website for a sample at [www.osbplf.org/services/resources/](https://www.osbplf.org/services/resources/) > Practice Aids > Technology and Data Management > Security and Data Breach. Save it in a common location accessible to all attorneys and staff, and mandate its use on all wire transfers. Ensure anyone involved in wire transfers is well-versed in the process. Inform your client and other involved parties that your firm follows strict wire transfer protocol. Regularly review and update the checklist for possible improvements.

## 8. TRUST YOUR INSTINCTS

Don't allow any sense of urgency to push you

to move quickly or to circumvent wire transfer protocol. Hackers prey on situations where a sense of urgency exists. Carefully follow protocol regardless of the circumstances.



Rachel Edwards is a PLF Practice Management Attorney.

## What to Do After a Wire Fraud

If you think you have been the victim of wire fraud, take the following actions:

- Immediately notify the involved banks of the fraud and request a claw-back of the funds.
- If you have PLF Excess Coverage, contact the Excess department during regular business hours at 503.639.6911 or email [excess@osbplf.org](mailto:excess@osbplf.org). If you have cyber or crime insurance through a commercial carrier, contact your carrier.
- Contact the police and FBI to report the fraud. You may also wish to file a complaint with the Federal Trade Commission.
- Contact the PLF at 503.639.6911 and ask to speak to a practice management attorney for additional information and resources. ■

### OTHER WORKS BY RACHEL EDWARDS

- “The Good Goodbye: Navigating Common Issues Facing Departing Associates,” *inBrief*, Issue 146, December 2024
- “Empower Yourself to Avoid the Risk of Failing to Know or Apply the Law,” *inBrief*, Issue 142, May 2023
- “eFiling and Service: Entry of Service Contact Information,” *inBrief*, Issue 141, October 2020

## PLF Cybersecurity Resources

- PLF CLEs ([osbplf.org](https://osbplf.org) > Services > CLEs & Resources > CLEs)
  - “How Law Firms Get Hacked (And What You Can Do About It)” (April 9, 2024)
  - “Understanding Your Firm’s Cybersecurity Obligations and Exposures” (May 31, 2023)
- *inBrief* ([osbplf.org](https://osbplf.org) > Services > CLEs & Resources > *inBrief* > June 2019 > “Cybersecurity and Employee Training”

## Sources

- “Multi-million dollar funds transfer fraud: A must read for all BC lawyers,” (<https://www.lif.ca> > About Us > What We Do > News > Notices to Lawyers)
- “Wire Fraud Scams on the Rise: 5 Tips to Reduce Your Risk,” (<https://www.practicepro.ca> > Archives > August 2022)
- “Heightened Discipline for Wire Fraud,” (<https://www.ncbar.org/members/resources/center-for-practice-management/blog/> > Keyword Search)



## Tips, Traps, and Resources

### OPEN SESAME: UNBLOCKING KEY EMAILS FROM SPAM FILTERS

Are you finding that emails from opposing counsel or the Bar are being blocked or failing to reach their intended recipients? Numerous factors may contribute to this issue; however, major email providers such as Yahoo, Outlook, and Google have strengthened their spam protection measures over this past year. Prevent crucial communications from slipping through the cracks with proactive strategies for ensuring email delivery and receipt. Here are simple yet essential tips to navigate common challenges.

**If you're not receiving expected emails**, you can update your settings to allow emails from specific domains, like @osbar.org or @osbplf.org. Add these domains to your safe sender list, or manually save the individual email addresses to your contacts. Some email providers streamline this process, allowing you to choose to have the addresses you've emailed added to your contacts

automatically. You can also set up filters or rules so emails from certain people go straight to your inbox or a designated folder. If issues persist, try sending an email to the person you're not receiving emails from to see if the problem resolves.

**If you're not sure the email you sent went through**, check your sent folder to confirm delivery. Sometimes, the recipient's email provider might block or bounce back your email without notification. If this happens, it's crucial to contact the individual to tell them about the problem, especially when providing electronic service. When serving a party via email, it's key to confirm proper service—you might need to reach out through multiple channels (like a follow-up phone call). To prevent your emails from being flagged as spam, personalize them whenever possible by adding the recipient's name and context of your email.

*Thank you to Monica Logan, PLF Practice Management Attorney, for this tip.*