☀ CAROUSEL

A Member who was recently employed by a research institution resigned from that position in mid-November. The Employee's decision to resign was based, in part, on the results of an independent, third-party review and assessment. Nearly one month after the Employee resigned, the Employer sent an email demanding that the Employee report to work, in-person. The Employer's reasons for sending this subsequent communication appear to be strategic.

On behalf of our Members, and for legal and other purposes, including various possible IP-related claims, it is important to clarify that November 15, 2024, is the effective date of the Employee's resignation. Accordingly, research beyond this date is not performed under *cover of authority* or in *furtherance of a legal or authorized purpose*. Research performed by or authorized by the Employer beyond November 15, 2024, is potentially subject to criminal prosecution.

With regard to any actual or potential infringement actions, please be advised that DEMARCATION is determined as per the effective date of the Demarcation Notice. In this case, a Demarcation Notice was issued to [REDACTED] on February 26, 2024, thus serving as the effective date of constructive notice.

A list of potential parties and/or claimants was previously provided to a representative of [REDACTED]. A list has also been sent to all Members and is otherwise available upon request.

NOTES & COMMENTARY:

An Employer cannot override the results of a Risk Review or overcome the consequences of a Risk Rating by demanding an action that would cause an Employee to directly violate the terms set forth in a Risk Mitigation Report. If an Employee has access to valid security-related information and makes personal security decisions on that basis, it is the Employer, not the Employee, who must Stand Down. Individuals, not Entities, are the first line of authority on all matters and decisions pertaining to an Individual Member's personal security.