

Best Practices for Protecting your Assets

Choate's four-part podcast series, "[Protecting your Assets](#)," addresses a variety of concerns at the intersection of employee departures and protecting valuable company trade secrets.

Consider the best practices below to help you navigate when you conduct exit interviews, mitigate database damage and stolen property, assess litigation concerning potential employee raids, and respond to demand letters:

Audit non-compete, confidentiality, and other contractual agreement

Ensure that you have electronic copies of all of the relevant signed agreements that you may want to enforce after an employee leaves. While existing agreements may be grandfathered under existing laws, revisiting these agreements before employees depart can help make sure that they are still enforceable.

Certify that all company property and documents have been returned

When an employee departs, have the employee sign a certification stating that all company property and documents have been returned. The certification may also require a search of personal files, such as personal email accounts.

Strike a healthy balance of employee access to data

To help ensure that your most critical data is protected, assess which employees need access to which levels of data. Then monitor network logs to make sure there is no unusual activity.

Conduct an exit interview

When an employee departs, confirm where the employee is going next. Then track the employee's moves with a formal reporting mechanism. This can help determine if multiple employees are leaving to join a competitor. In addition, when an employee leaves to join a competitor, remind the employee of any contractual and other obligations to your company.

Consider a forensic review

In some situations you may want to do more – such as where a critical group of employees leave to join a competitor, or where a departing employee may have provided false information during an exit interview. In those situations, conduct a forensic review of company devices to check for suspicious activity.

Institute investigation protocols

If your company receives a demand letter alleging misconduct, such as hiring an employee in violation of a non-compete, get prepared to conduct an effective investigation. Give careful consideration to the scope of the investigation, identify key stakeholders, and consider including both inside counsel (who can collect the starting set of information) and outside counsel (who may offer a fresh perspective).

For more information, please reach out to your Choate team or one of the following attorneys:



Michael Bunis
Practice Group Leader, IP Litigation
617-248-4030
mbunis@choate.com



Alison Reif
Practice Group Leader, Labor & Employment
617-248-5157
areif@choate.com



Adam Bookbinder
Partner, Government Enforcement & Compliance
617-248-4806
abookbinder@choate.com



Mark Edgerton
Partner, IP Litigation
617-248-5101
medgarton@choate.com



Anita Spieth
Partner, IP Litigation
617-248-4031
aspieth@choate.com



Greta Fails
Principal, IP Litigation
617-248-4039
gfails@choate.com



Lyndsey Kruger
Principal, Labor & Employment
617-248-4790
lkruger@choate.com



Listen to the “Protecting your Assets” podcast series

The information presented in this recording is for educational purposes only, it does not constitute legal advice for specific situations. If you wish to obtain legal advice, you should retain an attorney and explain the facts of your particular situation.