Confidentiality and Nondisclosure Agreements (CA)

MARK E. TERMAN, SUJATA P. WIESE AND SHAMAR J. TOMS-ANTHONY, DRINKER BIDDLE & REATH LLP, WITH PRACTICAL LAW COMMERCIAL TRANSACTIONS

A Practice Note discussing overall protection of a company's confidential information and the use of confidentiality agreements (also known as nondisclosure agreements or NDAs) in the context of commercial transactions under California law. It provides practical tips on developing internal systems and contract provisions designed to protect a company's sensitive information, including its business assets and relationships, data security, and trade secrets.

Nearly all businesses have valuable confidential information and, for many, confidential information is a dominant asset. Protection of confidential information within an organization is usually a vital business priority.

Companies also share, receive, and exchange confidential information with and from customers, suppliers, and other parties in the ordinary course of business and in a wide variety of commercial transactions and relationships. These transactions and relationships include when companies enter into:

- Consulting engagements.
- Service agreements.
- Strategic alliances.

Contractual confidentiality obligations are fundamental and necessary to help protect the parties that disclose information in these situations. Depending on the circumstances, these obligations can be documented in either:

- A free-standing confidentiality agreement (also known as a nondisclosure agreement or NDA), whether mutual (see, for example, Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA) (W-001-7616)) or unilateral (see, for example, Standard Document, Confidentiality Agreement: General (Short Form, Unilateral, Pro-Discloser) (CA) (W-012-7506)).
- Clauses within an agreement that covers a larger transaction (see Standard Clauses, General Contract Clauses: Confidentiality (Short Form) (CA) (W-000-0480) and General Contract Clauses: Confidentiality (Long Form) (CA) (W-000-0481)).

This Note describes:

- Considerations involved in safeguarding a company's confidential information and some common approaches and leading practices when using confidentiality agreements.
- Various forms of general confidentiality agreements and factors to consider in structuring specific agreements.
- Substantive provisions that are common to many commercial confidentiality agreements and issues that may be encountered when drafting, reviewing, and negotiating each clause
- Special considerations under California and federal law.

The practical considerations explained in this Note are also covered in checklist form in the Confidentiality and Nondisclosure Agreements Checklist (CA) (W-012-6092).

Specialized types of confidentiality agreements are used in connection with mergers and acquisitions (see Practice Note, Confidentiality Agreements: Mergers and Acquisitions (4-381-0514)) and certain finance transactions (see Practice Note, Confidentiality Agreements: Lending (1-383-5931)).

OVERALL PROTECTION OF CONFIDENTIAL INFORMATION

PROTECTING CONFIDENTIAL INFORMATION AS VALUABLE BUSINESS ASSETS

Most companies derive substantial value from their confidential information and data, both by having exclusive use of it in their own businesses and by sharing it selectively with customers, suppliers, and others. Confidential information can be used and shared more effectively and securely, to the greater benefit of the business, if the company routinely:

- Takes stock and assesses the value of its information assets.
- Maintains rigorous internal policies and practices to keep it confidential.

Confidential information takes various forms in different businesses and industries (see Definition of Confidential Information) and often includes information entrusted to a company by its customers, suppliers, and other parties, subject to contractual use restrictions and nondisclosure obligations.

COMPANY-WIDE INFORMATION AND DATA SECURITY POLICIES, SYSTEMS, AND PROCEDURES

Having effective confidentiality agreements in place with other parties is necessary but not sufficient to protect an organization's confidential information and data. Comprehensive protection requires the participation and coordination of management and staff at all levels across all functions, from finance and administration to marketing and sales. It often falls to the legal department, working closely with the information technology (IT) function and with the support of senior executives, to lead the company-wide information management and protection program.

Encryption, coupled with "need to know" access and other secrecy measures, can help keep information confidential. In California, encryption has been defined as "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security" (Cal Civ. Code § 1798.29(h)(4)).

Effective information and data security depends on developing comprehensive policies and procedures and applying them consistently. It is especially important to have in place:

- A uniform confidentiality and proprietary rights agreement that is to be signed by all employees as a condition of employment (see Standard Document, Employee Confidentiality and Proprietary Rights Agreement (CA) (3-518-4653)). Requiring that employees of companies with which the company does business (and has confidentiality agreements) sign confidentiality agreements can also be a sound part of a confidentiality program (see, for example, *GSI Tech., Inc. v. United Memories, Inc.*, 2015 WL 1802616, at *4 (N.D. Cal. Apr. 20, 2015) (unreported opinion)).
- An IT and communications systems policy that governs employees' appropriate use of these company resources, in the interest of protecting confidential information (see Standard Document, IT Resources and Communications Systems Policy (8-500-5003)).

Robust physical and electronic security measures should be implemented and regularly tested, audited, and updated as part of the larger effort to protect the company's information assets. The company should have:

- Systems and processes in place to monitor and detect unauthorized disclosures of confidential information.
- Contingency plans and procedures to address any leaks that are detected.

These procedures should include notification of other parties with information that may have been disclosed in violation of applicable confidentiality agreements and mandatory notification of individuals whose personal information is compromised (see Practice Note, Breach Notification (3-501-1474)).

Under California law, the format of a data breach notification should comply with specific requirements including:

- Mandatory title and headings.
- A design that calls attention to the "nature and significance" of the information contained.
- Minimum font size.

(Cal. Civ. Code § 1798.29(d).)

COMPLIANCE WITH CONTRACTUAL OBLIGATIONS GOVERNING OTHERS' CONFIDENTIAL INFORMATION

In addition to safeguarding their own confidential information, companies are responsible for protecting information that is disclosed to them by customers, suppliers, and others, as a matter of compliance with relevant confidentiality agreements or analogous provisions within larger commercial agreements.

The principal obligations (covenants) typically imposed on recipients of confidential information include:

- Nondisclosure obligations, including restrictions against further disclosure of the information to third parties (for example, to subcontractors).
- Restrictions on access to and use of the information within the recipient's business and among its employees.
- Physical and electronic security requirements, which may be more stringent than the recipient's policies and procedures applicable to its own confidential information.
- Obligations to return or destroy original materials containing confidential information and any printed or electronic copies made by the recipient, on expiration or termination of the applicable confidentiality agreement or provisions.

For more information on the principal obligations typically imposed on the recipients of confidential information, see Key Provisions and Issues.

TRADE SECRETS

Certain confidential business, financial, and technical information may be subject to protection as trade secrets under California law, in addition to and independent of any contractual protections afforded by confidentiality agreements or provisions. For example, any of the following types of information may be considered trade secrets if certain criteria are met:

- Client lists (see, for example, *Gordon v. Schwartz*, 147 Cal. App. 2d 213, 217 (1956)).
- Marketing plans.
- Pricing and discount structures.
- Unpatented inventions (see, for example, *Sketchley v. Lipkin*, 99 Cal. App. 2d 849, 854 (1950)).
- Business methods.
- Production processes.
- Product plans and designs (see, for example, *Vacco Indus., Inc. v. Van Den Berg*, 5 Cal. App. 4th 34, 50 (1992)).
- Recipes and chemical formulas (see, for example, *Brescia v. Angelin*, 172 Cal. App. 4th 133, 151 (2009)).
- Software algorithms and source code.

Other California cases have held that certain information is not subject to protection as a trade secret. For example, one court noted that source code generally is deemed a trade secret. However, the court distinguished, background information, such as business requirements and high level design specifications incorporated in released software and evident to the user in its operation is not protected by trade secret law. (*Agency Solutions.Com, LLC v. TriZetto Grp., Inc.*, 819 F. Supp. 2d 1001, 1017 (E.D. Cal. 2011).)

Another court found that training conducted by a radio station to give its traffic announcers a particular "quality, sound, and personality" was not a protectable trade secret. The court reasoned that specialized training given to employees to develop their subjective characteristics merely emphasized personal qualities, but was not part of the informational base belonging to the company. (*Metro Traffic Control, Inc. v. Shadow Traffic Network*, 22 Cal. App. 4th 853, 862-63 (1994) (description of trade secrets failed to describe information other than employees' ability to satisfy employer's requirements).)

Customer lists are not always protected. For example, in *American Paper & Packaging Products, Inc. v. Kirgan*, a customer list was not deemed a trade secret where the information was "generally known in the trade and already used by good faith competitors" (183 Cal. App. 3d 1318, 1326 (Cal. Ct. App. 1986)). The more difficult the list was to compile and the more detail that is attached to it (for example, customer history, whether an individual is a decision maker, preferences, and the like), typically the more likely the list is deemed a trade secret (see, for example, *Sun Distrib. Co., LLC v. Corbett*, 2018 WL 4951966, at *3-4 (S.D. Cal. Oct. 12, 2018). Business use of social media, such as LinkedIn, can make customer identity more readily known outside the company.

California, like nearly every state, offers some trade secret protection under its adopted version of the Uniform Trade Secrets Act. California has adopted a modified version of the Uniform Trade Secrets Act (CUTSA) (Cal. Civ. Code §§ 3426 to 3426.11; see State Q&A, Trade Secret Laws: California (8-504-5513)).

The CUTSA definition of "trade secret" includes virtually any information, such as a formula, pattern, compilation, program, device, method, technique, or process, if three basic components apply:

- The information is not generally known outside of the owner's organization and control.
- The owner derives economic value or business advantage by virtue of that secrecy.
- The owner makes reasonable efforts under the circumstances to preserve its secrecy.

(Cal. Civ. Code § 3426.1(d).)

Signed confidentiality agreements, coupled with need to know access and IT and other safeguards, can be important evidence of the third component. One court found that a company took reasonable steps to maintain the secrecy of certain information by requiring its employees to sign confidentiality agreements and acknowledgements that they had received and read the company's employee handbook, which outlined employee obligations regarding trade secret and confidential business information (*Pyro Spectaculars N., Inc. v. Souza*, 861 F. Supp. 2d 1079, 1091 (E.D. Cal. 2012)).

Defend Trade Secrets Act

As of May 2016, businesses may also find trade secret protection under the federal Defend Trade Secrets Act (DTSA) (18 U.S.C.A. §§ 1831 to 1839). The DTSA provides a federal cause of action for an owner of a trade secret that is misappropriated if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce (18 U.S.C.A. § 1836(b)(1)).

Under the DTSA, "trade secret" is defined as all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if both:

- The owner of the information has taken reasonable measures to keep it secret.
- The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

(18 U.S.C.A. § 1839(3).)

The DTSA does not preempt state trade secret laws (18 U.S.C.A. § 1838). For more information on trade secrets, see:

- Practice Notes:
  - Intellectual Property: Overview: Trade Secrets (8-383-4565); and
  - Protection of Employers' Trade Secrets and Confidential Information (5-501-1473).
- Standard Clause, General Contract Clauses, Confidentiality Agreement Clauses After the Defend Trade Secrets Act (W-002-9194).
- Defend Trade Secrets Act (DTSA) Issues and Remedies Checklist (W-003-6953).

PRIVACY AND DATA SECURITY LAWS AND REGULATIONS

Certain kinds of personal information commonly held by businesses, such as employee records and customers' financial accounts, may be subject to special protection requirements under various federal and state privacy and data security laws and regulations.

California law requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and protect the personal information from breach (Cal. Civ. Code § 1798.81.5(b)).

A person or business that conducts business in California is to notify a California resident if the person or business:

- Owns or licenses computerized data that includes the resident's personal information.
- Has learned of a breach in the security of the data and the information is:
  - unencrypted; or
  - encrypted and an encryption key or security credential that may permit reading or using the information has also

been or is reasonably believed to have been acquired by an unauthorized person.

(Cal. Civ. Code § 1798.82(a).)

These legal requirements are related to contractual nondisclosure obligations, but they apply whether or not the personal information is otherwise treated as confidential (see Practice Notes, US Privacy and Data Security Law: Overview (6-501-4555) and California Privacy and Data Security Law: Overview (6-597-4106)).

"Sensitive personal information" is a subset of personal information that is more significantly related to the notion of a reasonable expectation of privacy, and may include an individual's health-related or financial information.

There are federal and state statutes to protect specific types of personal information which certain business are obligated to follow, including:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, which cover certain health-related information (Pub. L. No. 104-191, 110 Stat. 1936 (1996); 45 C.F.R. §160.101, §162.100 and § 164.102).
- The Genetic Information Nondiscrimination Act, which applies specifically to genetic information (Pub. L. No. 110-233).
- The Fair and Accurate Credit Transaction Act designed to protect consumer credit information (15 U.S.C. §1681).
- California's Confidentiality of Medical Information Act (CMIA) (California Civil Code §§ 56 to 56.37), which is intended to protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider.
- Beginning January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100 to 1798.199) goes into effect. The bill, in part, grants a consumer the right to request a business to disclose the categories and specific pieces of information that it collects about the consumer. The bill is only applicable to businesses that meet specific requirements (for example, annual gross revenues in excess of $25 million), and it requires, among other things, that the business disclose the personal information collected, sold, or disclosed for a business purpose about a consumer. For more information, see Understanding the California Consumer Privacy Act (CCPA (W-017-4166)).

FORM AND STRUCTURE OF CONFIDENTIALITY AGREEMENTS

RELEVANT TRANSACTIONS AND RELATIONSHIPS

A range of commercial transactions and relationships involve either the disclosure of confidential information by one party to the other or a reciprocal exchange of information. Although many confidentiality agreements have similar structures and share key provisions, there is great variation in the form, structure, and substantive details that should be tailored to the specific circumstances of each agreement. For example, confidentiality agreements may be used when:

- Evaluating or engaging a business or marketing consultant or agency, where the hiring company is necessarily disclosing confidential information to enable the consultant to perform the assignment.
- Soliciting proposals from vendors, software developers, or other service providers, which usually involves the exchange of pricing, strategies, personnel records, business methods, technical specifications, and other confidential information of both parties.
- Entering into a co-marketing relationship, as an e-commerce business, with the operator of a complementary website or a similar type of strategic alliance.

WHY IS IT NECESSARY TO HAVE WRITTEN CONFIDENTIALITY AGREEMENTS?

Your business clients may not appreciate the importance of entering into written confidentiality agreements, preferring to rely on informal understandings and arrangements with parties to or from which confidential information is disclosed or received. However, there are numerous reasons to enter into written confidentiality agreements, such as:

- Avoiding confusion over what the parties consider to be confidential.
- Allowing more flexibility in defining what is confidential.
- Delineating expectations regarding treatment of confidential information between the parties, whether disclosing, receiving, or both disclosing and receiving confidential information.
- Enforcing written contracts is typically easier than oral agreements.
- Memorializing confidentiality agreements is often required under "upstream" agreements with third parties (for example, a service provider's customer agreement may require written confidentiality agreements with subcontractors).
- Maximizing protection of trade secrets, because under state law this protection can be weakened, or perhaps waived, if disclosed without a written agreement (see Trade Secrets).
- Covering issues that are indirectly related to confidentiality, such as non-solicitation (see General Provisions and Standard Clauses, Confidentiality Agreement: Non-Solicitation Clause (CA) (W-001-6417)).
- Maintaining standards that are expected of most commercial transactions and relationships.

STRUCTURE AND TIMING

A free-standing confidentiality agreement is sometimes the sole contractual arrangement that defines the parties' relationship. In other circumstances, it may be used as a preliminary document, intended either to co-exist with an eventual comprehensive agreement governing the larger transaction or to be superseded by separate confidentiality provisions in that agreement. A separate confidentiality agreement is often used:

- Where the parties need to exchange confidential information to request or prepare proposals for a larger transaction.
- To conduct due diligence in the course of negotiating a definitive agreement.

Confidentiality provisions are sometimes incorporated in a term sheet for certain kinds of deals but, because these clauses may be relatively lengthy, it may be easier to have them in a separate agreement. If the parties decide to include confidentiality provisions in the term sheet, they should ensure that all of the confidentiality provisions are binding, even if the other provisions are not. If the parties negotiate a term sheet after the signing

of a confidentiality agreement, it is a good idea to refer to the executed confidentiality agreement in the term sheet. Conversely, free-standing confidentiality agreements should reference any term sheets or definitive agreements that the parties contemplate, whether or not they supersede the confidentiality agreement. For more information on term sheets, see Practice Note, Term Sheets (5-380-6823).

The parties should sign a confidentiality agreement as early as possible in their relationship or at the outset of substantive negotiations in larger transactions, preferably before any confidential information is disclosed. If a party discloses information before signing the confidentiality agreement, the agreement should specifically cover prior disclosures.

MUTUAL, UNILATERAL, AND RECIPROCAL FORMS

Depending on the type of transaction or relationship, only one party may share its confidential information with the other or the parties may engage in a mutual or reciprocal exchange of information. There are distinct forms of confidentiality agreements to accommodate these different arrangements.

Unilateral Confidentiality Agreements

Unilateral confidentiality agreements contemplate that one of the parties intends to disclose confidential information to the other party, for example, where a consultant is to have access to the client's business information in the course of an engagement. In unilateral confidentiality agreements, the nondisclosure obligations and access and use restrictions apply only to the party that is the recipient of confidential information but the operative provisions can be drafted to favor either party. For sample unilateral confidentiality agreements, see Standard Documents, Confidentiality Agreement:

- General (Unilateral, Pro-Discloser) (9-501-6497).
- General (Unilateral, Pro-Recipient) (2-501-9258).

Mutual Confidentiality Agreements

In mutual confidentiality agreements, each party is treated as both a discloser of its and a recipient of the other party's confidential information (such as where two companies form a strategic marketing alliance). In these situations, both parties are subject to identical nondisclosure obligations and access and use restrictions for information disclosed by the other party. For a sample mutual confidentiality agreement, which can be used for general commercial relationships and transactions, see Standard Document, Confidentiality Agreement: General (Mutual) (1-501-7108). For a short form sample mutual confidentiality agreement, see Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA) (W-001-7616).

Even in transactions and relationships where the confidential information to be exchanged is not of equivalent kind or value, the parties may still agree to use a mutual confidentiality agreement. When preparing or reviewing a mutual confidentiality agreement under these circumstances, each party should consider whether it intends to primarily disclose or receive information and the relative value and sensitivity of the information to be exchanged and adjust the operative provisions accordingly. For example, an outsourcing customer should ensure that the definition of confidential information is as broad as possible and that the recipient is subject to strict nondisclosure obligations. However, the service provider may want a narrower definition and less restrictive obligations.

Reciprocal Confidentiality Agreements

In some circumstances, the parties may share certain confidential information with each other but not on a mutual basis. Instead of entering into a fully mutual confidentiality agreement, the parties enter into a reciprocal confidentiality agreement. Under this type of agreement:

- The scope and nature of the confidential information that each party intends to disclose is separately defined.
- The parties' respective nondisclosure obligations and access and use restrictions may differ accordingly.

For example, in a typical outsourcing transaction, the service provider may be required to disclose only limited technical information and pricing details to the customer, while the service provider is to be given extensive access to sensitive information about the customer's business methods and processes. In this situation, the customer may be especially concerned that this information is not shared with the service provider's other customers, which may be the customer's competitors.

LIMITATIONS AND RISKS OF CONFIDENTIALITY AGREEMENTS

Confidentiality agreements are very useful to prevent unauthorized disclosures of information but they have inherent limitations and risks, particularly when recipients have little intention of complying with them. These limitations include the following:

- Once information is wrongfully disclosed and becomes part of the public domain, it cannot later be "undisclosed."
- Proving a breach of a confidentiality agreement can be very difficult, particularly since most offenders will take steps to make their misuse of information difficult to detect and discover.
- Damages for breach of contract (or an accounting of profits, where the recipient has made commercial use of the information) may be the only legal remedy available once the information is disclosed. However, damages may not be adequate or may be difficult to ascertain, especially when the confidential information has potential future value as opposed to present value.
- Even where a recipient complies with all of the requirements under a confidentiality agreement, it may indirectly use the disclosed confidential information to its commercial advantage.

Remedies for breach of contract in California are generally limited. Often breach of confidentiality agreement claims are brought alongside other claims that offer broader remedies.

For example, unfair competition or unfair business practices claims can yield equitable relief including from injunction and turn-over orders, restitution, and disgorgement (Cal. Bus. & Prof. Code §§ 17200-17210).

If trade secrets are involved, trade secret claims generally displace statutory unfair competition and common law tort claims based on the same nucleus of facts (see *K.C. Multimedia, Inc. v. Bank of Am.*

Tech. & Operations, Inc., 171 Cal. App. 4th 939, 958-61 (2009)). Trade secret claims can provide:

- Broad injunctive relief.
- Economic recovery measured by:
  - actual loss;
  - unjust enrichment; or
  - reasonable royalty.
- Exemplary damages of up to two times the economic relief.
- Attorneys' fees.

(Cal. Civ. Code §§ 3426.2 to 3426.4.)

Election of remedies principles may make use of the confidentiality agreement as cornerstone evidence supporting non-contract claims more valuable than a breach of contract claim. California courts have made clear that breach of contract and the tort of breach of confidence are mutually exclusive causes of action, and that recovery for breach of contract precludes the availability of a tort cause of action (*Berkla v. Corel Corp.*, 302 F.3d 909, 918 (9th Cir. 2002)).

A California court found that a plaintiff failed to prove a breach of contract because it was not able to produce evidence demonstrating that it would have acquired new customers had the defendant not breached the confidentiality agreement. The plaintiff was required to show, with reasonable certainty, the loss of profit as a result of the defendant company's breach, and otherwise the award of damages would be entirely speculative. (*Urica, Inc. v. Pharmaplast S.A.E.*, 2013 WL 12123230, at *17-18 (C.D. Cal. May 6, 2013) (unreported opinion).)

On the other hand, in *Foster Poultry Farms, Inc. v. SunTrust Bank*, the Ninth Circuit Court of Appeals affirmed a lower court's decision to disgorge a defendant's profits (377 F. App'x 665 (9th Cir. 2010)). Rather than proving financial injury, the plaintiff proved that it suffered intangible harm and that the defendant and a competitor of the plaintiff were unjustly enriched from the breach of a confidentiality agreement (*Foster*, 377 F. App'x at 668-69).

Despite these limitations, the commercial benefits of disclosing the information under a confidentiality agreement normally outweigh the risks. To protect its confidential information most effectively, the disclosing party should carefully manage the disclosure process and have a contingency plan for responding to unauthorized disclosures by the recipient.

KEY PROVISIONS AND ISSUES

Confidentiality agreements, in their various forms, typically include the following key provisions:

- The persons or entities that are parties to the agreement (see Parties to the Agreement).
- The business purpose of the agreement (see Business Purpose).
- The definition of confidential information (see Definition of Confidential Information).
- What is excluded from the definition of confidential information (see Exclusions from the Definition).
- All nondisclosure obligations (see Nondisclosure Obligations).
- Any use and access restrictions (see Use and Access Restrictions).
- Any safekeeping and security requirements (see Safekeeping and Security Requirements).
- The agreement's term and the survival of nondisclosure obligations (see Term of Agreement and Survival of Nondisclosure Obligations).
- Any provisions relating to the return or destruction of confidential information (see Return or Destruction of Confidential Information).

PARTIES TO THE AGREEMENT

The parties to the agreement are the business entities or individuals that are exchanging confidential information and are subject to the security requirements, use restrictions, nondisclosure obligations, and the agreement's other operative provisions. Although only the parties themselves are bound by the agreement, consider whether:

- The parties' affiliates (including any parent and subsidiary entities) are the source of any of the confidential information to be shared under the agreement and whether any of them should be added as parties.
- Each party that is to be a recipient of confidential information may share it with its affiliates.
- The parties should be obligated to have employees and independent contractors who will have access to the information sign confidentiality and non-disclosure agreements.

A recipient party (and, if applicable, that party's affiliates) is also often permitted to share confidential information with its business, financial, and legal advisors and other representatives. Representatives typically include the recipient's:

- Officers, directors, employees, and other agents (such as shareholders or partners).
- Legal counsel.
- Accountants.
- Financial and tax advisors.

In some cases, the recipient party may prefer to have certain of its representatives enter into separate confidentiality agreements with the other party, rather than be held responsible for the representatives' compliance with the principal agreement.

For more information on permitting disclosure of confidential information to a party's representatives, see Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA): Disclosure and Use of Confidential Information (W-001-7616).

BUSINESS PURPOSE

Many confidentiality agreements limit the disclosure or exchange of confidential information to a specified business purpose, such as "to evaluate a potential marketing arrangement between the parties." A defined business purpose is especially useful as a basis for access and use restrictions in the agreement. For example, confidentiality agreements can restrict the disclosure of confidential information to the recipient, its affiliates, and representatives solely for use in connection with the stated purpose (see, for example, Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA): Section 1 (W-001-7616)).

Where a confidentiality agreement limited the use of confidential information to an ambiguous "Business Purpose," one California court broadly interpreted the receiving party's obligations so the party's actual use of the information was not allowed (*Urica, Inc. v. Medline Indus., Inc.*, 2011 WL 13128408, at *9 (C.D. Cal. Oct. 5, 2011) (unreported opinion)).

DEFINITION OF CONFIDENTIAL INFORMATION

Defining what information and data is confidential is central to any confidentiality agreement. Disclosing parties should:

- Ensure that confidential information is defined broadly enough to cover all of the information they (or their affiliates) may disclose, as well as any that may have been previously disclosed.
- Consider specifying the types of information that are defined as confidential information, to avoid the agreement being later deemed unenforceable because of an overly broad definition.

The types of information that are commonly defined as confidential include:

- Business and marketing plans, strategies, and programs.
- Financial budgets, projections, and results.
- Employee and contractor lists and records.
- Business methods and operating and production procedures.
- Technical, engineering, and scientific research, development, methodology, devices, and processes.
- Formulas and chemical compositions.
- Blueprints, designs, and drawings.
- Trade secrets and unpublished patent applications.
- Software development tools and documentation.
- Pricing, sales data, prospects and customer lists, and information.
- Supplier and vendor lists and information.
- Terms of commercial contracts.

In addition to business information that is actually disclosed or exchanged by the parties, confidential information may also include:

- Any information that a recipient derives from the discloser's confidential information. For example, a recipient may use confidential data in its financial projections.
- The fact that the parties are discussing and potentially entering into a particular relationship. It can be very damaging if a company's customers, competitors, or other interested parties find out about a deal before a formal announcement is made or the deal fails to close.
- The existence and terms of the confidentiality agreement itself.

Confidential information should include information entrusted to a party by its affiliates and by third parties, such as customers, which may itself be subject to "upstream" confidentiality agreements with the third parties (see, for example, Standard Clauses, General Contract Clauses: Confidentiality (Long Form) (CA): Section 1.1(d) (W-000-0481)).

The definition of confidential information should state the possible forms in which it may be disclosed (written, electronic, and oral) and whether the disclosed material is to be marked "confidential" or otherwise designated as confidential. Where especially sensitive or valuable confidential information is to be disclosed, numbered, printed copies may be distributed to specified individuals, so that all copies can be collected at the conclusion of the transaction (see Safekeeping and Security Requirements).

A California court held that there was no breach of a confidentiality agreement between parties when the express terms of the agreement provided that:

- Any tangible confidential information was to be marked "confidential."
- Any oral information was to be designated "confidential" before it was disclosed.

When the disclosing party failed to notify the receiving party that information was "confidential," the disclosing party was unable to demonstrate that the information was confidential and proprietary under the terms of the agreement. (*Hoffman v. Impact Confections, Inc.*, 544 F. Supp. 2d 1121, 1125-1126 (S.D. Cal. 2008).)

EXCLUSIONS FROM THE DEFINITION

Recipients should ensure there are appropriate exclusions from the definition (which can be broader or narrower, depending on the party). Typical exclusions include information that:

- Is or becomes public other than through a breach of the agreement by the recipient.
- Was already in the recipient's possession or was available to the recipient on a non-confidential basis before disclosure.
- Is lawfully received from a third party that is not bound by separate confidentiality obligations to the other party.
- Is independently developed by the recipient without using the confidential information.

NONDISCLOSURE OBLIGATIONS

Recipients of confidential information are generally subject to an affirmative duty to keep the information confidential and not to disclose it to third parties except as expressly permitted by the agreement. The recipient's duty is often tied to a specified standard of care.

For example, the agreement may require the recipient to maintain the confidentiality of the information using the same degree of care used to protect its own confidential information, but not less than a "reasonable" degree of care. The confidentiality agreement between parties before a California district court required the receiving party to exercise this standard of care. The court permitted the disclosing party's breach of contract claim to proceed when the disclosing party alleged that the receiving party had gained a competitive advantage by sharing product information with the receiving party's director of product management, rather than only those employees involved in the contemplated purpose. (*Silicon Image, Inc. v. Analogix Semiconductor*, 642 F. Supp. 2d 957, 963-65 (N.D. Cal. 2008).)

Recipients should ensure there are appropriate exceptions to the general nondisclosure obligations, including for disclosures:

- **To its representatives.** Most confidentiality agreements permit disclosure to specified representatives for the purpose of

evaluating the information and participating in negotiations of the principal agreement (see Parties to the Agreement).

- **Required by law.** Confidentiality agreements usually allow the recipient to disclose confidential information if required to do so by court order or other legal process. The recipient usually has to notify the disclosing party of this order (if legally permitted to do so) and cooperate with the disclosing party to obtain a protective order.

Disclosing parties commonly try to ensure that recipients are required to have "downstream" confidentiality agreements in place with any third parties, including affiliates, representatives, contractors, and subcontractors, to which later disclosure of confidential information is permitted. In these cases, either the recipient or the discloser may prefer to have these third parties enter into separate confidentiality agreements directly with the discloser.

USE AND ACCESS RESTRICTIONS

Apart from a recipient's nondisclosure obligations, confidentiality agreements typically limit access to and use of the information even within the recipient's organization. For example, access and use may be restricted to the recipient's employees who have a "need to know" the information solely for the defined business purpose.

SAFEKEEPING AND SECURITY REQUIREMENTS

Recipients may be required to adopt specific physical and network security methods and procedures to safeguard the discloser's confidential information. Some agreements require that confidential information be segregated in a "data room," with a log of all internal access and third-party disclosures. Recipients may also be obligated to notify the disclosing party of any security breaches or unauthorized disclosures.

California law requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures, protect the personal information from breach, and notify the resident in the event of a breach (Cal. Civ. Code §§ 1798.81.5(b) and 1798.82(a) and see Privacy and Data Security Laws and Regulations).

Certain business and personal information in regulated industries, such as healthcare and financial, should also be kept confidential.

Best practices for protecting such confidential information include:

- Controlling access to digitally stored information by using passwords, firewalls, and encryption.
- Disposing of sensitive paper documents by shredding them or using a confidential waste bin.
- Keeping confidential paper documents in lockable document storage cabinets. For an added level of protection, the lockable storage cabinet can be kept in a locked room that has limited access.
- Providing training to employees about protecting confidential information.

TERM OF AGREEMENT AND SURVIVAL OF NONDISCLOSURE OBLIGATIONS

Confidentiality agreements can run indefinitely, covering the parties' disclosures of confidential information at any time, or can terminate on a certain date or event, such as the:

- Conclusion of the defined business purpose.
- Signing of a principal agreement.

Whether or not the overall agreement has a definite term, the parties' nondisclosure obligations can be stated to survive for a set period, running for some number of years from the date on which information is actually disclosed. Survival periods of one to five years are common.

Disclosing parties typically prefer an indefinite period while recipients generally favor a fixed term. The term often depends on the type of information involved and how quickly the information changes. Some information becomes obsolete fairly quickly, such as marketing strategies or pricing arrangements. Other information may need to remain confidential long into the future, such as:

- Customer lists.
- Certain technology and technical information.
- Business methods.

Having too short a term can undermine both the effectiveness of the agreement and ongoing reasonable owner efforts to protect trade secrets, which are a factor in whether information qualifies for trade secret status (see Trade Secrets).

California courts have indicated that they will enforce perpetual confidentiality agreements that are aimed to protect trade secrets (see *Silicon Image, Inc. v. Analogix Semiconductor, Inc.*, 2008 WL 166950, at *17 (N.D. Cal. Jan. 17, 2008) (unreported opinion)).

RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION

Disclosing parties should ensure they have rights to the return of their confidential information on termination of the confidentiality agreement or at any time on their request.

Recipients often want the option to destroy the confidential information instead of returning it to the disclosing party. In the course of evaluating the other party's confidential information, conducting due diligence, or negotiating a principal agreement, a recipient may combine its own confidential information with that of the discloser. In that situation, the recipient usually wants to destroy the information because returning it means disclosing its own confidential information. Disclosing parties usually allow this destruction option but often require the recipient to certify in writing that the information was in fact destroyed. Disclosing parties should be especially aware of this risk because there is no way for a disclosing party to be sure that a recipient has destroyed the information.

It is often not practical for a recipient to certify that all confidential information has been destroyed, due to the widespread use of automated network back-up programs and e-mail archive systems. For this reason, a recipient may try to include language that allows archival copies to be retained (see, for example, Standard Clauses, General Contract Clauses: Confidentiality (Long Form) (CA): Section 1.4(c) (W-000-0481)). This issue is usually fact specific and should be negotiated between the parties.

Recipients also try to include language that allows them to keep copies of confidential information for evidentiary purposes or if

required to do so by law or professional standards. Disclosing parties agree to this but sometimes require that the recipients' outside attorneys keep the copies to protect against abuses.

GENERAL PROVISIONS

Confidentiality agreements may also include any of the following general provisions.

Intellectual Property Rights

Confidentiality agreements typically provide that the disclosing party retains any and all of its intellectual property rights in the confidential information that it discloses and disclaim any grant of a license to the recipient (see, for example, Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA): Section 6 (W-001-7616)). While the primary focus of this practice note is not agreements with employees, practitioners should not overlook California Labor Code Section 2870 and related Labor Code sections, addressing the unenforceability of certain provisions in employee invention assignment agreements (Cal. Lab. Code §§ 2870-2872).

Warranty Disclaimers

It is common for the disclosing party to disclaim all warranties on the accuracy and completeness of its confidential information (see, for example, Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA): Section 5 (W-001-7616)).

No Further Obligations

Each party may want to expressly state that it has no obligation to enter into any transaction beyond the confidentiality agreement itself (see, for example, Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA): Section 5 (W-001-7616)).

Non-Solicitation

In some situations, confidentiality agreements prohibit one or both parties from soliciting or offering employment to the other party's employees. Some non-solicitation provisions also prohibit establishing relationships with customers and suppliers of the other party. These provisions should be narrowly drafted to avoid potential enforceability issues and, particularly in California, may be unenforceable if drafted more broadly. For example, parties wishing to add customer and supplier non-solicitation language should consider limiting it to specifically prohibit solicitation through the use of trade secret information or other unlawful means (see *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 1526 (1997)).

In California, Business and Professions Code Section 16600 (Section 16600) voids contract provisions that restrain anyone from engaging in a lawful profession, trade, or business (Cal. Bus. & Prof. Code § 16600).

Section 16600 generally blocks agreements between commercial parties not to hire away the other's employees (see, for example, *VL Sys., Inc. v. Unisen, Inc.*, 152 Cal. App. 4th 708, 718 (2007) (broad no-hire provision between commercial parties was unenforceable under California law) and *Thomas Weisel Partners LLC v. BNP Paribas*, 2010 WL 546497, at *6 (N.D. Cal. Feb. 10, 2010) (no-hire agreement was unenforceable under Section 16600 to the extent that it prohibited an ex-employee from hiring or assisting to hire former coworkers for one year after the end of his employment)).

Recently, California law related to the enforceability of employee non-solicitation (as opposed to no-hire) agreements may be evolving.

Many courts have followed the approach of the 1985 decision *Loral Corp. v. Moyes*, that an employee non-solicitation agreement is not necessarily void on its face and is enforceable if a court deems it reasonable (174 Cal. App. 3d 268, 279 (1985)).

In *Loral*, a former officer of a company had entered into a termination agreement with it which restrained him from disrupting, damaging, impairing, or interfering with the company's business by interfering with or raiding its employees. The court determined that the enforceability of this "noninterference" agreement depended on its reasonableness, evaluated in terms of:

- The employer.
- The employee.
- The public.

The court held that, applying this standard, the agreement was not void on its face under Section 16600. Employees were free to look for and accept employment with the former officer's new company and only could not be contacted first by him. The purpose of the agreement presumably was to maintain a stable work force and it had no overall negative impact on trade or business. (*Loral*, 174 Cal. App. 3d at 279-80.)

The California Supreme Court, analyzing a **customer** non-solicitation provision in the 2008 decision *Edwards v. Arthur Andersen LLP*, found that a reasonableness standard conflicts with the plain language of Section 16600. The court held that the agreement was void under Section 16600. (44 Cal. 4th 937, 946-48 (2008).) However, *Edwards* expressly did not reach the question of the enforceability of an **employee** non-solicitation provision (*Edwards*, 44 Cal. 4th at 946 n.4).

In the 2018 decision *AMN Healthcare, Inc. v. Aya Healthcare Servs., Inc.*, the court expressed doubt about the continued viability of *Loral* post-*Edwards*, but also rested its reasoning on the particular facts of the *AMN* case. The *AMN* defendants' **business** was recruiting and placing medical professionals and an employee non-solicitation provision therefore restrained them from engaging in their profession. The court held that the provision was void under Section 16600. (28 Cal. App. 5th 923, 939 (Cal. Ct. App. 2018); see also *Barker v. Insight Glob., LLC*, 2019 WL 176260, at *3 (N.D. Cal. Jan. 11, 2019) (following *AMN*, plaintiff's motion for reconsideration granted in a decision also relating to a company providing staffing services) and see *Barker v. Insight Glob., LLC*, 2018 WL 3548911 (N.D. Cal. July 24, 2018).)

Non-solicitation provisions are disfavored in California and should be drafted cautiously, with close attention to evolving state law and precedent (see Standard Clauses, Confidentiality Agreement: Non-Solicitation Clause (CA) (W-001-6417)). Counsel should pay particular attention to enforceability concerns (for example, whether the client might be subject to unfair business practice allegations if the language is found unenforceable) (see *Application Grp., Inc. v. Hunter Grp., Inc.*, 61 Cal. App. 4th 881, 908 (1998)).

Announcements and Publicity

As an exception to parties' nondisclosure obligations, there may be a provision permitting either or both parties to announce or publicize the fact or terms of their relationship, usually subject to prior approval by the other party (see, for example, Standard Clause, General Contracts Clauses: Public Announcements (2-523-8703)).

Equitable Relief

To mitigate the potential consequences of unauthorized disclosures, confidentiality agreements often include an acknowledgement that a disclosing party should be entitled to injunctive relief to stop further disclosure of the confidential information, in addition to monetary damages and other remedies (see, for example, Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA): Section 8 (W-001-7616)). Injunctive relief is available in California to enforce a confidentiality agreement (see, for example, *Imi-Tech Corp. v. Gagliani*, 691 F. Supp. 214, 229-30 (S.D. Cal. 1986); Cal. Civ. Code § 3426.2(a) and see *ReadyLink Healthcare v. Cotton*, 126 Cal. App. 4th 1006, 1018 (2005)).

Indemnification

In addition to the right to seek equitable relief, disclosing parties sometimes try to include an indemnification provision holding the recipient responsible for all costs relating to the enforcement of the agreement. Recipients typically resist this language. A typical compromise is to have the losing side in any dispute pay the winner's fees and expenses, including legal fees (see Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (CA): Equitable Relief (W-001-7616)).

Governing Law, Jurisdiction, and Venue

State laws vary on the validity and enforceability of certain provisions in confidentiality agreements, such as the allowable duration of nondisclosure obligations and the scope of non-solicitation provisions. Each party should consult with counsel qualified in the state before entering into a confidentiality agreement governed by the laws of California. For sample governing law, jurisdiction, and venue provisions, see Standard Clauses, General Contract Clauses: Choice of Law (CA) (W-000-0276) and Choice of Forum (CA) (W-000-0274).

For confidentiality provisions in employment agreements, as of January 1, 2017, California law limits an employer's ability to require its employees to enter into agreements that include out-of-state choice of law or forum selection clauses by making them voidable by the employee unless the employee was represented by independent counsel (Cal. Lab. Code § 925).

02-19