Confidentiality and Nondisclosure Agreements (CO)

JONATHAN B. BOONIN AND JUSTIN C. KONRAD, HUTCHINSON BLACK AND COOK, LLC, WITH PRACTICAL LAW COMMERCIAL TRANSACTIONS

Search the Resource ID numbers in blue on Westlaw for more.

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 Colorado 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.
- Supply contracts.
- Distribution agreements.

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) (5-535-7285)) or unilateral (see, for example, Standard Document, Confidentiality Agreement: General (Short Form, Unilateral, Pro-Discloser) (W-000-1570)).
- Clauses within an agreement that covers a larger transaction (see Standard Clauses, General Contract Clauses: Confidentiality (Short Form) (CO) (W-000-1569) and Confidentiality (Long Form) (CO) (6-501-7380)).

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 Colorado and federal law.

The practical considerations explained in this Note are also covered in checklist form in the Confidentiality and Nondisclosure Agreements Checklist (4-381-0514).

Specialized types of confidentiality agreements are used in connection with mergers and acquisitions (see Practice Note, Confidentiality Agreements: Mergers and Acquisitions) () 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 (see, for example, *Branta, LLC v. Newfield Prod. Co.,* 2017 WL 1435882, at *5 (D. Colo. Apr. 24, 2017) (confidentiality agreement between parties in an oil and gas transaction)).

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.

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 must be signed by all employees as a condition of employment (see Standard Document, Employee Confidentiality and Proprietary Rights Agreement (CO) (W-000-9993)). While courts may not entirely rely on confidentiality and proprietary rights agreements in evaluating trade secret disputes, they are an important factor (see, for example, *L-3 Commc'ns Corp. v. Jaxon Eng'g & Maint., Inc.*, 125 F. Supp. 3d 1155, 1181 (D. Colo. 2015)).
- 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)). Technological security measures that courts may consider in evaluating trade secret disputes include encryption, password-protection, and policies of limited or "need to know" access (see, for example, *Saturn Sys., Inc. v. Militare*, 252 P.3d 516, 522 (Colo. App. 2011)).

Robust physical and electronic security measures must be implemented and regularly tested, audited, and updated as part of the larger effort to protect the company's information assets (see Practice Note, Trade Secret Audits (W-019-2129)). 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)). In Colorado, data breaches are governed by the Colorado Consumer Protection Act (Colo. Rev. Stat. Ann. § 6-1-716). For more information on data breach notification in Colorado, see State Q&A, Data Breach Notification Laws: Colorado (3-578-9365).

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 Colorado law, in addition to and independent of any contractual protections afforded by confidentiality agreements or provisions. For example, courts have found the following types of information trade secrets:

- Customer lists, sourcing information, research and development efforts, and marketing strategies (*R & D Bus. Sys. v. Xerox Corp.*, 152 F.R.D. 195, 197 (D. Colo. 1993); but see *Gas Prod. Corp. v. BTU Mktg., LLC*, 2017 WL 4222619, at *7 (D. Colo. Sept. 22, 2017) (customer lists ascertainable from public sources are not trade secrets)).
- A bid price on a contract (*Ovation Plumbing, Inc. v. Furton*, 33 P.3d 1221, 1224 (Colo. App. 2001)).
- Software, even when it incorporates elements that are in the public domain (*Rivendell Forest Prod., Ltd. v. Georgia-Pac. Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994)).
- An instructional program (*Harvey Barnett, Inc. v. Shidler*, 338 F.3d 1125, 1129-1132 (10th Cir. 2003).
- Business Methods (*SGS Acquisition Co. v. Linsley*, 352 F. Supp. 3d 1109, 1121-22 (D. Colo. 2018)).
- Production processes (*Port-a-Pour, Inc. v. Peak Innovations, Inc.*, 49 F. Supp. 3d 841, 862 (D. Colo. 2014)).
- Recipes and chemical formulas (*Nat. Miracles, Inc. v. Team Nat., Inc.*, 2009 WL 3234386, at *3 (D. Colo. Oct. 1, 2009)).

Colorado Uniform Trade Secrets Act

Additionally, Colorado, like nearly every state, offers some trade secret protection under its adopted version of the Uniform Trade Secrets Act (UTSA) referred to as the Colorado Uniform Trade Secrets Act (CUTSA) (Colo. Rev. Stat. Ann. §§ 7-74-101 to 7-74-110; see State Q&A, Trade Secret Laws: Colorado: Significant Differences Between Adopted Version and the Model UTSA (9-506-3323)). For an overview of the UTSA, see Practice Note, Protection of Employers' Trade Secrets and Confidential Information: Trade Secrets (5-501-1473).

The CUTSA defines trade secrets as:

- The whole or portion of:
  - scientific or technical information;
  - designs;
  - processes;
  - procedures;
  - formulas;
  - improvements;
  - confidential business or financial information;
  - listing of names, addresses, or telephone numbers; and
  - Any other information that is secret and of value.
- The subject of measures taken by the owner to prevent the secret from becoming available to people beyond those granted permission by the owner.

(Colo. Rev. Stat. Ann. § 7-74-102(4); see also (Gold Messenger, Inc. v. McGuay, 937 P.2d 907, 911 (Colo. App. 1997).)

In addition to the statutory factors, Colorado courts consider six common law factors when evaluating whether information qualifies as a trade secret:

- The extent to which it is known outside the business.
- The extent to which it is known to employees and others within the business.
- The precautions taken by the trade secret's holder to guard the secrecy of the information.
- The savings and value to the holder or to a competitor.
- The cost or effort expended in obtaining and developing the information.
- The cost or time it would take for others to acquire or copy the information.

(*Colorado Supply Co. v. Stewart*, 797 P.2d 1303, 1306 (Colo. App. 1990); *Network Telecommunications, Inc. v. Boor-Crepeau*, 790 P.2d 901, 903 (Colo. App. 1990); *Hertz v. Luzenac Grp.*, 576 F.3d 1103, 1108 (10th Cir. 2009).)

CUTSA violators are subject to injunctions and monetary damages, including:

- Compensatory damages,
- Exemplary damages.
- Attorneys' fees.

(See, for example, *Atlas Biologicals, Inc. v. Kutrubes*, 2019 WL 4594274, at *17 (D. Colo. Sept. 23, 2019)).

Colorado's criminal trade secret theft statute uses the same definition of trade secret as the CUTSA (Colo. Rev. Stat. Ann. §§ 7-74-102(4) and 18-4-408(2)(d)).

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)). Often, parties bring suit under both the DTSA and the CUTSA (see, for example, *Arctic Energy Servs., LLC v. Neal*, 2018 WL 1010939, at *1 (D. Colo. Feb. 22, 2018)).

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. § 1839(3).)

The DTSA does not preempt state trade secret laws, and injunctions under the DTSA may not conflict with state law prohibiting restraints on the practice of a lawful profession, trade, or business. 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.

For example, Colorado's consumer protection statute requires that businesses develop a written destruction policy if it maintains records containing personal identifying information, which includes:

- Social Security numbers.
- Personal identification numbers.

- Passwords and passcodes.
- Official state or government-issued driver's license or identification card number.
- A passport number.
- Biometric data.
- Employer, student, or military identification number.
- Financial transaction device.

(Colo. Rev. Stat. Ann. §§ 6-1-713(1), 6-1-716(1)(a) (defining biometric data), and 18-5-701(3) (defining financial transaction device).)

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 Note, US Privacy and Data Security Law: Overview (6-501-4555)).

Data privacy laws and regimes usually extend protections to personal information of employees, customer, and clients.

Broadly, the term personal information (also known as "personally identifiable information" or "personal data"), refers to information that can be used to identify, locate, or contact an individual, alone or when combined with other personal or identifying information. Colorado law defines personally identifiable information (see Privacy and Data Security Laws and Regulations).

For US federal and state privacy and data security laws, the precise definition of personal information varies depending on the specific jurisdiction and law, and may be more narrowly defined. For more information, see Practice Note, US Privacy and Data Security Law: Overview (6-501-4555).

"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 information or financial information.

In general, businesses must implement internal policies and procedures to safeguard personal information. Encryption is one example of a method included in some privacy laws to protect such information, keeping in mind that sensitive personal information should be given enhanced protection. Employers in particular must also note that data privacy obligations are not only to protect active employees, but extend to protect any non-employee groups such as clients and customers, job applicants, consultants, independent contractors, and terminated or retired employees.

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

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, which covers 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 Transactions Act designed to protect consumer credit information (15 U.S.C.A. § 1681).
- The Colorado Consumer Protection Act (Colo. Rev. Stat. Ann. §§ 6-1-713, 6-1-713.5, and 6-1-715).

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 lost (deemed 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 (8-524-3805)).
- 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 intends 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-Recipient) (2-501-9258) and General (Unilateral, Pro-Discloser) (9-501-6497).
- General (Short Form, Unilateral, Pro-Recipient) (3-532-3908) and General (Short Form, Unilateral, Pro-Discloser) (5-535-7285).

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) (0-539-6425).

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.
- 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 (see, for example, *Q-Tech Labs. Pty Ltd. v. Walker*, 2002 WL 1331897, at *14 (D. Colo. June 4, 2002) (plaintiff denied monetary damages for lack of evidence)).

- Even where a recipient complies with all of a confidentiality agreement's requirements, it may indirectly use the disclosed confidential information to its commercial advantage.

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 dealing with 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 (see, for example, *Cont'l Credit Corp. v. Garcia*, 2016 WL 614475, at *4 (D. Colo. Feb. 16, 2016) (denying the terms of a confidentiality agreement were sufficiently ambiguous to apply to affiliated entities)).
- 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): Disclosure and Use of Confidential Information (0-539-6425).

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, *Port-a-Pour,* 49 F. Supp. 3d at 861-62 (D. Colo. 2014) (enforcing a confidentiality agreement restricting use of intellectual property and trade secrets for manufacture and sale of products in a designated territory, per a limited-duration license agreement)).

For an example of a business purpose clause, see Standard Document, Confidentiality Agreement: General (Short Form, Mutual): Section 1 (0-539-6425).

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.
- 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) (CO): Section 1.1(d) (W-000-1569)).

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 must 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).

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.

Colorado courts look to whether the measures are reasonable under the circumstances. For example, a federal court analyzing Colorado law found a party took reasonable measures to protect a trade secret when it:

- Posted signs warning employees to keep certain information confidential.
- Required employees to sign confidentiality agreements.
- Barred visitors from viewing production processes.
- Marked certain documents as confidential.
- Required contractors to sign confidentiality agreements.

(*Hertz v. Luzenac Grp.*, 576 F.3d 1103, 1112 (10th Cir. 2009); see also *Colorado Supply Co., Inc. v. Stewart*, 797 P.2d 1303, 1306 (Colo. Ct. App. 1990).)

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.

Many industries and companies have best practices for safeguarding confidential information, including the adoption of identity assurance and credential management with each level representing a different degree of certainty in the identity of the user. Other requirements may relate to the use of mobile devices and encrypting stored electronic 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. In Colorado, survival periods of one to five years are typical.

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 technical information.
- Business methods.

The disclosing party must be careful when including term limits in confidentiality agreements involving trade secrets to avoid undermining efforts to maintain trade secret status. While Colorado courts have not directly addressed the issue, a court may find the expiration of a confidentiality obligation of a limited duration as evidence that the trade secret owner is not exercising reasonable efforts to maintain the secrecy of the information (see *Structured Capital Sols., LLC v. Commerzbank AG*, 177 F. Supp. 3d 816, 835 (S.D.N.Y. 2016); *DB Riley, Inc. v. AB Eng'g Corp.*, 977 F. Supp. 84, 90-91 (D. Mass. 1997); *Alta Devices, Inc. v. LG Elecs., Inc.*, 343 F. Supp. 3d 868, 878 (N.D. Cal. 2018) (the fact that a contract expired does not automatically render any information incapable of receiving trade secret protection, but it is a fact that may be considered to determine whether trade secrets were adequately protected)).

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) (CO): Section 1.4(c) (W-000-1569)). 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): Section 6 (0-539-6425)).
- **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): Section 5 (0-539-6425)).
- **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): Section 5 (0-539-6425)).
- **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 must be narrowly drafted to avoid potential restraints on trade, and may be unenforceable if drafted more broadly than reasonably necessary to protect a party's interests (see, for example, Standard Clauses, Confidentiality Agreement: Non-Solicitation Clause (8-524-3805)). They may also violate Colorado's law against non-competition covenants, which, when between employers and employees in the state, are contrary to public policy and void, with the exception of:
  - Contracts for the purchase and sale of a business or its assets.
  - Trade secret protection.
  - Contracts providing for recovery of expenses from training, in certain circumstances.
  - Executive and management personnel and officers and employees who constitute their professional staff.
- (Colo. Rev. Stat. Ann. § 8-2-113(2), see also *Saturn Sys., Inc. v. Militare*, 252 P.3d 516, 526 (Colo. App. 2011) (non-solicitation agreement is enforceable to protect trade secrets if reasonably limited in time and scope) and *Cont'l Credit Corp. v. Dragovich*, 2013 WL 3303976, at *4 (D. Colo. July 1, 2013) (analyzing trade secret and management exceptions)).
- **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): Section 8 (0-539-6425)). CUTSA provides for temporary and final injunctive relief for actual or threatened misappropriation of trade secrets (Colo. Rev. Stat. Ann. § 7-74-103).

- **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): Equitable Relief (0-539-6425)).
- **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 Colorado. For sample governing law, jurisdiction, and venue provisions, see Standard Clauses, General Contract Clauses: Choice of Law (CO) (W-000-1963) and Choice of Forum (CO) (W-000-1778).