Confidentiality and Nondisclosure Agreements (PA)

PAUL J. GRECO, BUCHANAN INGERSOLL & ROONEY PC, WITH PRACTICAL LAW COMMERCIAL TRANSACTIONS

Search the Resource ID numbers in blue on Practical Law for more.

This Practice Note discusses 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 Pennsylvania 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:

- 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) (see Standard Document, Confidentiality Agreement: General (Short Form, Mutual) (0-539-6425)).
- Clauses within an agreement that covers a larger transaction (see Standard Clauses, General Contract Clauses: Confidentiality (Short Form) (PA) (w-000-0660) and General Contract Clauses: Confidentiality (Long Form) (PA) (w-000-0659)).

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.

The practical considerations explained in this Note are also covered in checklist form in the Confidentiality and Nondisclosure Agreements Checklist (6-501-7380).

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. Cases in Pennsylvania often note that the parties have entered into a contractual relationship that prevents the use or disclosure of confidential information of a party's customers, vendors, pricing, and business strategies and methods. See, for example:

- *Ecolaire Inc. v. Crissman*, 542 F. Supp. 196, 198-99, 208 (E.D. Pa. 1982) (applying Pennsylvania law, the court enforced agreements to maintain the confidentiality of information relating to business methods, pricing, products, and sales and operations).
- *Fleisher v. Bergman*, 2014 WL 10965754 at *1, *6 (Pa. Super. Mar. 31, 2014) (the court holding that there was a clear right to relief from a breach of agreement not to use or disclose marketing strategies, customer lists, pricing policies, professional methods and means, and names of vendors and dealers).

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 (PA) (6-607-8570)). When evaluating whether certain types of information are protectable as trade secrets, Pennsylvania courts consider the existence of confidentiality agreements as a factor to help guide their determination about whether a party takes reasonable measures to maintain the secrecy of the information. See, for example:
  - *Alpha Pro Tech, Inc. v. VWR International LLC*, 984 F. Supp. 2d 425, 437-38 (E.D. Pa. 2013) (the court applying Pennsylvania law and holding that determining whether a party took sufficient steps to safeguard proprietary information requires consideration of the existence of confidentiality agreements); and
  - *Den-Tal-Ez, Inc. v. Siemens Capital Corp.*, 566 A.2d 1214, 1230 (Pa. Super. 1989) (stating that the employer's use of confidentiality agreements with research and sales personnel supported the finding of trade secrets).
- 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 and Communications Systems Policy (8-500-5003)). Pennsylvania courts consider the existence of corporate policies requiring the use of password protected databases as evidence of whether a party has taken reasonable steps to safeguard confidential information. See, for example:
  - *A.M. Skier Agency, Inc. v. Gold*, 747 A.2d 936, 941 (Pa. Super. 2000) (stating that the fact that the employer required the use of a password protected database supported conclusion that the employer took reasonable steps to protect information); and
  - *Bimbo Bakeries USA, Inc. v. Botticella*, 2010 WL 571774 at *10 (E.D. Pa. Feb. 9, 2010), *aff'd* 613 F.3d 102 (3d Cir. 2010) (applying Pennsylvania law, the court found that a party took reasonable measures to protect information where it restricted access to and compartmentalized confidential information on its servers and entered into confidentiality agreements with its employees).

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. 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 Pennsylvania, the Breach of Personal Information Notification Act (73 P.S. § 2301 et seq.) provides standards for the notifications that are necessary when a security breach occurs (73 P.S. §§ 2303 and 2305) (see Privacy and Data Security Laws and Regulations).

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 Pennsylvania law, in addition to and independent of any contractual protections afforded by confidentiality agreements or provisions. Confidential information and trade secrets are not necessarily the same and may refer to entirely different bodies of information under Pennsylvania law (*Den-Tal-Ez,* 566 A.2d at 1224). While both protect legitimate business interests, certain confidential information may only be protected by agreement because, while confidential to a business, the information does not qualify for protection under the law as a trade secret (see *Den-Tal-Ez*, 566 A.2d at 1224). Any of the following types of information may be considered trade secrets if certain criteria are met:

- Client lists.
- Marketing plans.
- Pricing and discount structures.
- Business methods.
- Production processes.
- Recipes and chemical formulas.
- Software algorithms and source code.

At common law, Pennsylvania courts utilized a definition of trade secrets that is set forth in the Restatement of Torts § 757, which provides that a "trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and gives him an opportunity to obtain an advantage over competitors who do not know or use it" (Restatement of Torts § 757, comment b (adopted in *Felmlee v. Lockett*, 351 A.2d 273, 277 (Pa. 1976)). This common law definition of trade secret is substantially similar to the definition of "trade secret" that Pennsylvania adopted when it passed the Pennsylvania Uniform Trade Secrets Act.

Applying this general definition, Pennsylvania courts consider a list of factors to evaluate whether any specific type of information actually qualifies as a trade secret, including:

- The extent to which the information is known outside the owner's business.
- The extent to which the information is known by employees and others involved in the owner's business.
- The extent of the measures taken by the owner to guard the secrecy of the information.
- The value of the information to the owner and to the owner's competitors.
- The amount of effort or money expended by the owner in developing the information.
- The ease or difficulty with which the information could be properly acquired or duplicated by others.

(*Tyson Metal Products, Inc. v. McCann*, 546 A.2d 119, 121 (Pa. Super. 1988).)

Where these factors tend to favor the existence of trade secrets, Pennsylvania courts have found a wide variety of information to qualify as a trade secret, including:

- Scientific data, product designs, formulas, and manufacturing processes. For example:
  - *Bimbo Bakeries*, 2010 WL 571774 at *10 (holding that formulas, designs, and processes for making products are trade secrets);
  - *SI Handling Systems, Inc. v. Heisley*, 753 F.2d 1244, 1257-58 (3d Cir. 1985) (recognizing that technical data, if secret, may be protected as trade secret under Pennsylvania law); and
  - *Harry Miller Corp. v. Mancuso Chems. Ltd.*, 469 F. Supp. 2d 303, 311 (E.D. Pa. 2007) (holding that a chemical product's formula constituted a trade secret).
- Business information, strategic and marketing plans or tools, and pricing information. For example:
  - *Air Products & Chemicals v. Johnson*, 442 A.2d 1114, 1121-22 (Pa. Super. 1982) (holding that the status of negotiations with customers, proposed plant configurations and methods of delivery as well as analysis of market opportunities all constituted trade secrets);
  - *Bimbo Bakeries*, 2010 WL 571774 at *10 (holding that strategies for increasing profits, promotional strategies, and business information about matters such as plant closures and costs all constituted trade secrets);
  - *Fisher Bioservices, Inc. v. Bilcare, Inc.*, 2006 WL 1517382 at *16 (E.D. Pa. May 31, 2006) (stating that pricing information is protectable as a trade secret);
  - *Exl Labs., LLC v. Egolf*, 2010 WL 5000835, at *6 (E.D. Pa., Dec. 7, 2010) (finding the substance of unique incentive and rebate programs and pricing information for products and services qualified as trade secrets); and
  - *Home Line Furniture Indus., Inc. v. Banner Retail Mktg.*, 630 F. Supp. 2d 527, 540-41 (E.D. Pa. 2009) (recognizing a unique internet-based marketing tool as a protectable trade secret).
- Customer information which is not easily replicated and is created through significant investment of resources. For example:
  - *Bro-Tech Corp. v. Thermax*, 651 F. Supp. 2d 378, 409-10 (E.D. Pa. 2009) (stating that a compilation of customer data may qualify as a trade secret if it is not readily obtainable from another source and was generated in such a fashion that it constitutes intellectual property of the owner);
  - *Morgan's Home Equipment Corp. v. Martucci*, 136 A.2d 838, 842 (Pa. 1957) (stating that customer lists and customer information which have been compiled with a material investment of time and money can be trade secrets); and
  - *O.D. Anderson Inc. v. Cricks*, 815 A.2d 1063, 1072-73 (Pa. Super. 2003) (stating that customer lists may constitute trade secrets).
- However, Pennsylvania courts do not apply trade secret status to customer list information where that information is readily available from other sources (see, for example, *Brett Senior & Assocs. v. Fitzgerald*, 2007 WL 2043377, *6 (E.D. Pa. Jul. 13, 2007) (holding that customer lists may be entitled to protection as trade secrets, but are at "the very periphery of the law" and not protectable as such when the information is readily obtained from another source); see also *Pestco, Inc. v. Associated Prods., Inc.*, 880 A.2d 700, 707 (Pa. Super. Ct. 2005) (holding that equity will not protect names and addresses that are easily ascertainable by observation)).
- Computer programs (see, for example, *Chmura v. Deegan*, 581 A.2d 592, 592-93 (Pa. Super. 1990) (the court affirming an injunction

granted to protect computer programs used to embroider designs on clothing as trade secrets)).

- Combinations of the above (see, for example, *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, *8 (W.D. Pa. Dec. 13, 2007) (finding business information relating to the development, marketing, and sale of a product and customer communications protectable as trade secrets).

Pennsylvania Uniform Trade Secrets Act

Additionally, Pennsylvania, like nearly every state, offers some trade secret protection under its adopted version of the Uniform Trade Secrets Act. Pennsylvania has adopted a slightly modified version of the Uniform Trade Secrets Act (PUTSA) (12 Pa. C.S.A. §§ 5301 et seq.); see State Q&A, Trade Secret Laws: Pennsylvania (9-508-2227)).

The PUTSA states three general conditions for the protection of information as trade secrets:

- The information is not generally known or ascertainable outside of the owner's organization and control.
- The owner derives economic value or business advantage by having exclusive use of the information.
- The owner makes reasonable efforts to preserve its secrecy.

The PUTSA defines a trade secret as information, including a formula, drawing, pattern, compilation including a customer list program, device, method, technique or process that both:

- Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

(12 Pa. C.S.A. § 5302.)

The PUTSA differs slightly from the UTSA in the following ways:

- In defining trade secrets, the PUTSA contains explicit references to a "customer list" along with a "program, device, method, technique or process" that meets the foregoing criteria (12 Pa. C.S.A. § 5302). The UTSA contains no such references.
- For the purpose of determining whether exemplary damages are available for an act of misappropriation, the PUTSA includes a definition of the phrase "willful and malicious" (12 Pa. C.S.A. § 5302) (defining "willful and malicious" as such intentional or gross neglect as to evince a reckless indifference to the rights of others and an entire want of care that raises a presumption that wrongdoer is conscious of the consequences of his actions). The UTSA does not include a similar definition.

Currently, Pennsylvania courts apply the factors described above to evaluate whether the particular type of information at issue qualifies for trade secret status, as they did under common law (see *Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102, 109 (3d Cir. 2010); see also *Iron Age Corp. v. Dvorak*, 880 A.2d 657, 663 (Pa. Super. Ct. 2005) (applying the factors to hold that trade secrets do not include any of a worker's aptitude, skill, dexterity, or manual and mental ability)).

The crucial factors for determining whether certain information constitutes a trade secret under Pennsylvania law are:

- Substantial secrecy.
- Competitive value to the owner.

(*Brubaker Kitchens, Inc. v. Brown*, 2006 WL 1193223, at *1 (E.D. Pa. May 3, 2006) (quoting *O.D. Anderson, Inc. v. Cricks*, 815 A.2d 1063, 1070 (Pa.Super.Ct.2003).)

When evaluating whether reasonable efforts have been made to protect the substantial secrecy of information, confidentiality agreements continue to play an important role in satisfying that requirement (see, for example, *Alpha Pro Tech*, 984 F. Supp. 2d at 437-38 (the court, applying Pennsylvania law, holding that ascertaining whether a party took sufficient steps to safeguard proprietary information requires the consideration of the existence of confidentiality agreements)).

Pennsylvania also has a criminal trade secrets theft statute that defines a trade secret as all or any portion of any:

- Scientific or technical information.
- Design.
- Process.
- Procedure.
- Formula.
- Improvement.

(18 Pa. C.S.A. § 3930(e).)

Further, the above items must be:

- Valuable.
- Specifically identified by the owner as of a confidential character.
- Unpublished or have not otherwise become public knowledge.

(18 Pa. C.S.A. § 3930(e).)

The criminal trade secret statute contains a rebuttable presumption that scientific or technical information has not been published or otherwise become a matter of general public knowledge when the owner has taken measures to prevent it from becoming available to unauthorized persons (18 Pa. C.S.A. § 3930(e)).

Defend Trade Secrets Act

As of May 2016, businesses may also find trade secret protection under the federal Defend Trade Secrets Act (DTSA). 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 of service used in, or intended for use in, interstate of foreign commerce (18 U.S.C. §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 has taken reasonable measures to keep such information 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, 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 Note, Intellectual Property: Overview: Trade Secrets (8-383-4565) and Standard Clause, General Contract Clauses, Confidentiality Agreement Clauses After the Defend Trade Secrets Act (w-002-9194).

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. In Pennsylvania, these statutes include:

- The Breach of Personal Information Notification Act (73 P.S. § 2301 et seq.). This Act requires an entity that maintains, stores, or manages computerized data which includes personal information to provide notice of any breach of the data's security system after discovering the breach without unreasonable delay.
- The Confidentiality of HIV-Related Information Act (35 P.S. § 7601 et seq.). This Act prohibits the disclosure of another person's HIV-related information without consent.
- The Pennsylvania Drug and Alcohol Abuse Control Act (71 P.S. § 1690.101 et seq.). This Act requires confidential treatment of patient records and other information prepared or maintained by county-based prevention, intervention, and treatment programs for drug and alcohol abuse.
- The Mental Health Procedures Act (50 P.S. § 7101 et seq.). This Act prohibits the disclosure of another person's treatment for a mental health condition without consent.
- Privacy of Social Security Numbers (74 P.S. § 201). This statute prohibits the disclosure of Social Security information.

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)).

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 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) (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.

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, in which the scope and nature of the confidential information that each party intends to disclose is separately defined and their 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:
  - *Den-Tal-Ez,* 566 A.2d at 1233 (noting that injuries flowing from a threatened breach of a confidentiality agreement "are precisely the types of harm that are not subject to exact valuation and compensation through damage awards");
  - *Ecolaire Inc.,* 542 F. Supp. at 205 (recognizing the difficulty of proving damages for breach of a confidentiality agreement, Pennsylvania courts have readily found that a threatened breach of a confidentiality agreement warrants a finding of irreparable injury sufficient to support a request for injunctive relief);
  - *Omicron Systems, Inc. v. Weiner*, 860 A.2d 554, 564-65 (Pa. Super. 2004) (a Pennsylvania court endorsed using a liquidated damages clause as an appropriate measure of damages once the breach has occurred); and
  - *Fishkin v. Susquehanna Partners, G.P.*, 2007 WL 560703 at *6 (E.D. Pa. Feb. 12, 2007) (the court stating that Pennsylvania does not permit disgorgement of the defendant's profits as a remedy for breach of contract or as an appropriate measure of the plaintiff's damages).

- 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.
- Each party that is to be a recipient of confidential information may share it with its affiliates.

Pennsylvania law generally respects the corporate form as it relates to liabilities that arise out of the conduct of business. The Pennsylvania Supreme Court has held in a different context that separate corporations retain their distinct identities notwithstanding the fact that they may have common stockholders, directors, and officers (see *Shelburne Sportswear Inc. v. City of Philadelphia*, 220 A.2d 798, 203 (Pa. 1966) (holding that the tendency is not to disregard corporate individuality)). Although there may be legal theories pursuant to which one company may be bound by the contractual obligations of another, best practice is to utilize separate agreements with each entity that is to bound by the terms of a confidentiality agreement.

In Pennsylvania, the receiving party's obligation under a confidentiality agreement may turn on where they acquired the information. For example, a court found that a contract between a distributor and manufacturer did not prohibit the distributor from using, publishing, or disclosing confidential information belonging to the manufacturer that it received from a third party. Although the third party may have owed confidentiality obligations to the manufacturer, the contract protected only information disclosed by parties to each other. (*Alpha Pro Tech*, 984 F.Supp.2d at 444-45.)

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. See, for example:

- *Joseph L. Brooks Mfg. Corp. v. GSC Electronics, Ltd.*, 1982 WL 52143 at *2, *6 (E.D. Pa. Mar. 30, 1982) (an agreement's recitation that it was being entered into as part of the parties' discussion of royalty and manufacturing rights was later relied upon by the court for the purpose of concluding that an enforceable contract existed which limited the use of information to purposes that were for parties' joint benefit).
- *Den-Tal-Ez*, 566 A.2d at 1219, 1231-1232 (the court granting an injunction to foreclose the potential use of confidential information that an agreement prohibited the receiving party from using for its own purposes).
- *Morgan Truck Body, LLC v. Fredrickson Distribution LLC*, 2013 WL 4766331 at *3, *5-*6 (E.D. Pa. Sept. 5, 2013) (non-disclosure agreement that defined "Authorized Use" of confidential information was an enforceable contract).

Confidentiality agreements can also 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): 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.

Although the parties may define the scope of confidential information in an agreement, Pennsylvania courts may disregard an overly broad definition where evidence is presented that the information in question is, in fact, publicly available (see, for example, *Iron Age*, 880 A.2d at 664 (the court refusing to accord trade secret status to a customer list despite the terms of a confidentiality agreement where evidence showed that identities of customers in industry were widely known)).

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) (PA): Section 1.1(d) (w-000-0659)).

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 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.

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.

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 typical, although Pennsylvania courts may shorten the length of the restricted period if the evidence reflects that the information to be protected loses its value or become stale more quickly than the confidentiality agreement envisions. For example, one court noted that a confidentiality agreement prohibited use of disclosed information for five years from receipt, but uphold an injunction limited to three years "during which the usefulness of the information can reasonably be anticipated to dissipate" (see *Den-Tal-Ez*, 566 A.2d at 1221, 1233).

Disclosing parties typically prefer an indefinite period while recipients generally favor a fixed term. Pennsylvania courts will not refuse to enforce a confidentiality agreement simply because the period restricting disclosure is indefinite (see, for example, *Morgan Truck Body,* 2013 WL 4766331 at *6, (the court refusing to dismiss a claim for breach of a confidentiality agreement based on the contention that the agreement had terminated, noting that the express terms of the agreement provided that the restrictions survived termination)). 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.

Whether any particular type of information can be protected as either a trade secret or as confidential information and how long the restraint may remain enforceable are both fact sensitive inquiries under Pennsylvania law. A Pennsylvania court has provided that:

- The particular character of the information is not relevant under Pennsylvania law.
- Pennsylvania law does not limit protection to information that is purely technical in nature, but rather affords protection to a wide-range of commercial information.
- The crucial indicia appear to be substantial secrecy and competitive value to the owner.
- The length of a restraint that is set forth in a non-disclosure agreement may be adjusted by the court to be consistent with the time period for which the information retains its secret nature and value. The scope of an injunction is dependent upon the "nature and reasonably expected 'life' of the information."
- Pennsylvania law recognizes that issues relating to the confidential character of the information and its value to the owner are necessarily to be made on a case-by-case basis.

(see *Den-Tal-Ez*, 566 A.2d at 1228-33.)

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) (PA): Section 1.4(c) (w-000-0659)). 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)).

The enforceability of non-solicitation or "no-hire" provisions in confidentiality agreements that are part of commercial transactions is not settled law in Pennsylvania. The issue was addressed in *GeoDecisions v. Data Transfer Solutions, LLC*, 2010 WL 5014514, at *3 (M.D. Pa. Dec. 3, 2010), and the court specifically noted the absence of Pennsylvania precedent.

In *GeoDecisions*, two companies entered into a confidentiality agreement as part of an effort to collaborate on particular project. The agreement provided that neither company could solicit the other's personnel for employment for a period of two years from the date of the agreement. When the defendant subsequently breached this commitment, the plaintiff sued and sought an injunction. In determining whether injunctive relief was available, the district court first considered whether the agreement was valid and enforceable. The district court characterized a no-hire clause as a restraint on trade that is typically held to be void under Pennsylvania law, unless the restraint is:

- Ancillary to the main purpose of a lawful transaction.
- Necessary to protect a party's legitimate interest.
- Supported by consideration.
- Reasonably limited in time and territory.

(*GeoDecisions*, 2010 WL 5014514 at *4.)

In *GeoDecisions*, the district court concluded that all four requirements were met and that the no-hire clause was enforceable. Although the *GeoDecisions* case is instructive, there are no decisions by Pennsylvania's appellate courts resolving the same issues. Thus, the validity of non-solicitation or no-hire clauses in confidentiality agreements is not settled law in Pennsylvania at this time.

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)). Pennsylvania courts recognize that the potential disclosure of confidential information creates a risk of injury that would be difficult to measure or remedy by a damages award, making injunctive relief appropriate. See, for example:

- *Den-Tal-Ez*, 566 A.2d at 1232-33 (the threatened disclosure of confidential information is precisely the type of injury that most warrants injunctive relief).
- *Ecolaire Inc.,* 542 F. Supp. at 205 (the use of confidential information constitutes irreparable harm and supports the issuance of an injunction).

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 Pennsylvania. For sample governing law, jurisdiction, and venue provisions, see Standard Clauses, General Contract Clauses: Choice of Law (PA) (w-000-0227) and Choice of Forum (PA) (w-000-0225).

Choice of law, venue, and jurisdiction clauses can be enforced in Pennsylvania. Pennsylvania courts generally honor the intent of the contracting parties and enforce choice of law provisions in contracts they execute (see *Kruzits v. Okuma Machine Tool, Inc.*, 40 F.3d 52, 55 (3d Cir. 1994)) (*citing Smith v. Commonwealth National Bank*, 557 A.2d 775, 777 (Pa. Super. 1990)). Where the validity of the choice of law clause is challenged, Pennsylvania courts apply the tests set forth in the Restatement (Second) of Conflict of Laws § 187. These tests, which tend to impose a heavy burden on the party seeking to invalidate a choice of law clause, provide that:

- The parties' chosen law will govern their contractual rights and duties if the particular issue is one which they could have resolved through an explicit provision in their agreement.
- If the parties could not have agreed (for example, if one of the parties lacked the capacity to contract or if the contract is illegal), then the chosen law will still govern unless the chosen state has

no substantial relationship to the parties or their transaction or if the chosen law is contrary to a fundamental policy of a state with a materially greater interest in the resolution of the dispute.

(See *Kruzits*, 40 F.3d at 55.)

Pennsylvania courts also generally enforce venue and jurisdiction clauses. The Pennsylvania Supreme Court has long held that forum selection clauses are presumed to be valid (see *Central Contracting Co. v. C.E. Youngdahl & Co.*, 209 A.2d 810, 816 (Pa. 1965)). The Pennsylvania Superior Court has held that forum selection clauses will be deemed unenforceable only when:

- The clause itself was induced by fraud or overreaching.
- The forum selected in the clause itself is so unfair or inconvenient that a party, for all practical purposes, will be deprived of an opportunity to be heard.
- The clause is found to violate public policy.

(See *Patriot Commercial Leasing Co., Inc. v. Kremer Restaurant*, 915 A.2d 647, 651 (Pa. Super. 2006).)

Because forum selection clauses also typically include a consent to jurisdiction in the chosen forum, jurisdiction clauses do not require separate analysis. If the forum selection clause is valid, the consent to jurisdiction will be similarly upheld (see *DePuy Synthes Sales, Inc. v. Edwards*, 23 F. Supp. 3d 472, 480 (E.D. Pa. 2014)).

09-17