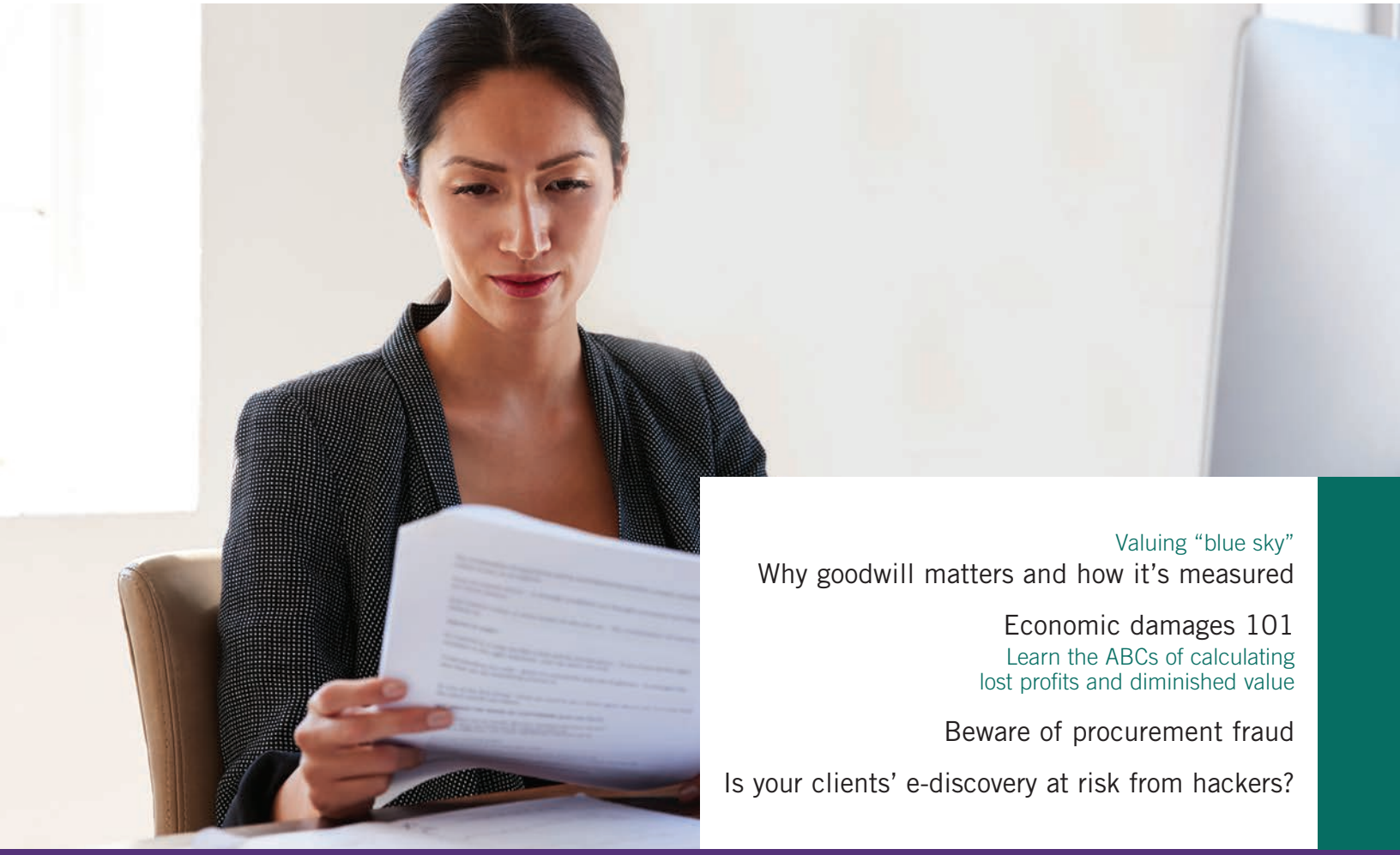
JANUARY / FEBRUARY 2018

ADVOCATE'S EDGE



Valuing "blue sky"
Why goodwill matters and how it's measured

Economic damages 101
Learn the ABCs of calculating lost profits and diminished value

Beware of procurement fraud

Is your clients' e-discovery at risk from hackers?

Valuing "blue sky"

Why goodwill matters and how it's measured

Goodwill is an indefinite-lived intangible asset. Some businesses have no goodwill. For others, goodwill is a significant part of their value. It comes into play in various business valuation assignments, from divorce and shareholder litigation to business combinations and financial reporting. Not surprisingly, the purpose of a valuation assignment can affect how it's measured.

In a nutshell

Goodwill can be hard to define. Examples of the way goodwill can be viewed include:

1. Going concern value. This comes from business assets that are producing income. The assemblage of capital (financial resources and equipment), labor and management creates intangible value.

2. Excess business income. This is the amount of business income that exceeds the amount necessary to provide a fair rate of return on tangible assets (for example, buildings and equipment) and identifiable intangible assets (for example, patents, trademarks, copyrights, trade secrets, franchises and licenses). The theory is that such excess income is due to goodwill.

3. Expectation of future economic benefits. The third component arises from expected economic benefits that aren't directly related to current assets or operations. The value is the net present value of income that will come from expectations of attracting new customers, developing new goods or services and participating in M&As.

How much is goodwill worth? Parties — and experts — seldom agree on the value of this intangible or the appropriate valuation technique to apply.

Under GAAP

Under U.S. Generally Accepted Accounting Principles (GAAP), goodwill normally goes unreported on the balance sheet unless it's purchased, as in the sale of a business. The term "goodwill" refers to the residual asset recognized in a business combination after all other identifiable tangible and intangible assets acquired and liabilities assumed have been recognized. GAAP requires goodwill to be carried on the books at its initial fair value less any impairment. It generally isn't subject to amortization.

Goodwill is impaired if the implied fair value of goodwill of a reporting unit (basically, an operating unit with its own discrete financial information, separate from the overall company) drops to an

What's the difference between personal and business goodwill?

In divorce cases in most states, it's not enough to value goodwill as a whole. Your valuation expert also might need to break it down between personal and business goodwill. Why? Because some states specifically exclude *personal* goodwill from the marital estate.

Personal (or professional) goodwill is linked to individual business owners and their abilities to generate future income. It often attaches to a professional person because of confidence in that person's skills and credentials, but the courts in some jurisdictions have rules that owners of manufacturing and retail businesses can also generate personal goodwill. Personal goodwill typically can't be transferred to a third party unless the seller enters into a postclosing consulting or employment agreement with the buyer.

Conversely, *business* (or enterprise) goodwill arises from factors that separate it from the skills or attributes of an individual owner of the business. Examples of these factors include the company's location, assembled workforce, brands, patents and name. Business goodwill is generally easier to transfer to a third party buyer than personal goodwill.

To ensure proper treatment of goodwill, it's imperative to review the statutes and case law in the applicable jurisdiction of the divorce action.

amount less than its carrying amount, or book value, including any deferred income taxes. Most companies are required to test for impairment at least annually, and more frequently under certain conditions.

Private companies can elect out of impairment testing, and, instead, amortize goodwill over a period not to exceed 10 years. But they're still required to test for impairment if a "triggering event" — such as the loss of a major customer or the enactment of an adverse government regulation — occurs.

In divorce cases

How goodwill is handled in a divorce context varies depending on state laws and the facts of the case. When the marital estate includes a private business interest, most states include some or all goodwill when divvying up the couple's assets. In a few states, all goodwill is specifically *excluded* from the marital estate.

Often, the treatment of goodwill in divorce cases hinges on whether a spouse who doesn't participate in the business (the noncontrolling spouse) will receive alimony based on the earning capacity of the spouse that will retain the business (the controlling spouse). The logic here is known as "double dipping." That is, the noncontrolling spouse shouldn't benefit twice from the same asset by receiving 1) alimony based on the controlling spouse's salary, and 2) half of the fair value of goodwill or, in some states, personal goodwill. (See "What's the difference between personal and business goodwill?" above.)

A critical factor in valuing goodwill is whether the controlling spouse's salary is *reasonable* compared to what other people receive for performing comparable work elsewhere. If the controlling spouse is under- or overpaid, adjustments to the amount of alimony awarded and income stream that's used to value the business may be warranted.

Goodwill hunting

Different circumstances call for different approaches to valuing goodwill. Whether you're valuing goodwill for financial reporting or litigation purposes, retaining a qualified professional will ensure you get a value you can count on. ■

Economic damages 101

Learn the ABCs of calculating lost profits and diminished value

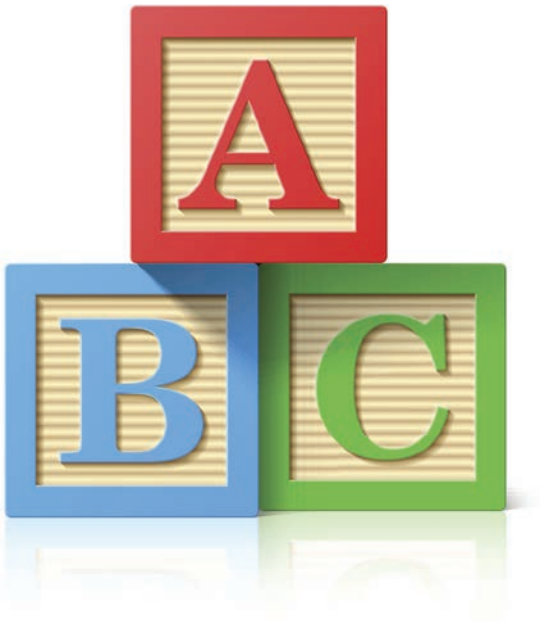
The ultimate goal of any economic damages case is to make the plaintiff "whole" again. In other words, the expert needs to answer the question: Where would the plaintiff be today "but for" the defendant's alleged wrongdoing? Many factors go into this assessment. Economic damages may include lost profits, diminished business value or both.

What methods are commonly used?

When business valuation experts calculate economic damages they generally rely on the following methods:

Before-and-after. Here, the expert assumes that, if it hadn't been for the breach or other tortious act, the company's operating trends would have continued in pace with past performance. In other words, damages equal the difference between expected and actual performance. A similar approach quantifies damages as the difference between the company's value before and after the alleged tort occurred.

Yardstick. Under this technique, the expert benchmarks a damaged company's performance to external sources, such as publicly traded comparables or industry guidelines. The presumption is that the company's performance would have mimicked that of its competitors if not for the tortious act.



Sales projection. Projections or forecasts of the company's expected cash flow serve as the basis for damages under this method. Damages involving niche players and start-ups often call for the sales projection method, because they have limited operating history and few meaningful comparables.

> Most jurisdictions hold plaintiffs at least partially responsible for mitigating their own damages.

An expert considers the specific circumstances of the case to determine the appropriate valuation method (or methods) for that particular situation.

What's next?

After experts have estimated lost profits, they discount their estimates to present value. Some jurisdictions have prescribed discount rates, but, in many instances, appraisers subjectively build up the discount rate based on their professional opinions about risk. Small differences in the discount rate can generate large differences in valuators' final conclusions. As a result, the subjective discount rate is often a contentious issue.

The final step is to address mitigating factors. What could the damaged party have done to minimize its loss? Most jurisdictions hold plaintiffs at least partially responsible for mitigating their own damages. Similar to discount rates, this subjective adjustment often triggers widely divergent opinions among the parties involved.

What are some common pitfalls to avoid?

Some key factors need to be considered to avoid over- or underestimating a damaged business's loss. For example, the taxation of damages can have a significant impact on an expert's conclusion. Indeed, many damages awards are taxable. If the plaintiff must pay taxes, an after-tax assessment would *not* be equitable. Also realize that some parts of a damages award, such as return of capital, may be nontaxable and require an after-tax estimate.

Taxes also need to be handled properly when lost profits are discounted to present value. In other words, if damages need to be calculated on a pre-tax basis, the expert should use pretax discount rates. Mismatching after-tax discount rates to pre-tax cash flows would overstate damages, all else being equal.

In addition, it's important to not assume that damages will occur into perpetuity. Economic damages generally occur over a *finite* period. That is, they have a beginning and an end. Eventually most plaintiffs can overcome the effects of the defendant's alleged wrongdoing.

If time and budgets permit, allow your expert an opportunity to review the opposing expert's analyses. He or she may find that the opposition didn't take into account one or more of these key factors.

Need help?

Plaintiffs suffer economic damages from many commercial torts, including breach of contract, patent infringement and commercial negligence. Hire an experienced business valuation professional to help calculate lost profits and business value with confidence. These objective experts are familiar with proven techniques that can withstand a *Daubert* challenge and know how to avoid potential pitfalls. ■

Beware of procurement fraud

Scams involving vendors and suppliers are among the most prevalent — and potentially damaging — types of fraud facing your clients today. You can reduce losses by helping business clients identify procurement frauds and take critical steps to detect and prevent them.

Common schemes

Common types of procurement fraud include:

Overbilling. Perpetrators can misuse invoices in several ways. For example, they might submit inflated invoices for goods and services. The price could exceed the agreed-upon price or reflect charges for more items than the company received. A vendor also could change the date on a legitimate invoice and resubmit it for multiple payments.

Bid rigging. Bid rigging occurs when two or more competing vendors conspire against a company. In a bid *rotation* scheme, vendors all submit bids but take turns as the low bidder. In a bid *suppression* scheme, vendors agree that one or more will

withdraw a submitted bid — or just not bid for the company's contract — to ensure that a particular bid is accepted.

Complementary bid rigging has the same goal but works differently. Competing vendors submit bids with excessively high prices or other terms that will cause them to be rejected.

Kickbacks. Vendors can pay company employees to facilitate the payment of a fraudulent invoice or secure a contract. Typically, the invoice or contract incorporates the amount of the kickback, meaning the company gets hit twice.

Protective measures

Proactive business owners take steps to minimize their risk of procurement fraud. Internal controls, a company's first line of defense against fraud, can be fortified to reduce the opportunity for dishonest people to commit procurement schemes.

> Internal controls, a company's first line of defense against fraud, can be fortified to reduce the opportunity for dishonest people to commit procurement schemes.

For example, a business might segregate accounting duties to ensure that employees who process invoices don't also process payments or receive and reconcile bank statements. Or a business can establish an anonymous fraud hotline for employees, vendors and customers to report suspicious behavior and other red flags.

A company might also screen its vendors and suppliers, verifying the business's name, IRS Form W-9, tax identification number, state business registration, telephone number, address, bank account and internal contact. Any changes in vendor or supplier profiles (along with duplicate payments) require further investigation.

Likewise, background checks should be conducted on employees who 1) order materials and supplies, and 2) pay or approve vendor and supplier invoices. And their mailing addresses can be cross-checked against vendor and supplier mailing addresses to search for any overlap.

Data mining can facilitate these verification procedures. This technology uses software to do targeted analyses of entire data populations. When it comes to fraud detection, companies can employ trend analysis to identify thresholds that, if exceeded, issue an alert triggering further investigation.

For example, a vendor's average payment amount or the median amount paid per vendor each month can serve as a guideline. If a payment exceeds the average by, say, $10,000 or 10%, the system could trigger an alert that management needs to verify the transaction. Companies also can set up alerts for payments 1) just under limits that would require a manager's approval before payment, 2) in round dollar amounts, 3) with checks or invoice numbers out of sequence, and 4) where the address for delivery of goods differs from the payment address.

Where there's smoke …

Procurement fraud often hits companies hard and fast. When a client suspects something is amiss, a qualified forensic accounting expert can help them respond swiftly and effectively. ■

Is your clients' e-discovery at risk from hackers?

News headlines seem to report a new hacking scandal every week. Hackers don't target just businesses and government agencies — increasingly, they're realizing the potential treasure troves to be accessed through law firms' IT systems.

Recognizing the risks

Electronic data, including confidential financial and accounting information, is commonplace in discovery today. But the prevalence of e-discovery has also created vulnerabilities. Law firms can inadvertently provide one-stop shopping for hackers, whether these criminals seek information to use in litigation, to gain a competitive advantage in the marketplace or to hold for ransom.

Think about it: Litigation usually involves some of your clients' most valuable information. Discovery may involve the gathering of clients' trade secrets, financial or employee records, customer information, protected personal information, and other types of privileged or sensitive information stored in electronic form.

Once it's given to your law firm, this information might subsequently be sent to clients, colleagues, law firms, third-party vendors and the same parties on the opposing side. It could transfer via unencrypted email, file sharing or cloud services, DVDs, and hard drives.

These paths of access often lack appropriate security precautions, making them all potential points of attack. And information "at rest" isn't any safer — data sitting in repositories hasn't necessarily been reviewed for, or purged of, protected materials. Hackers know that repositories contain information that can be valuable even if it's not relevant to a case.

Safeguarding data

Law firms need to act now to put appropriate security measures in place. At a minimum, you should:

- Limit the amount of information shared and authorized access to it,
- Use a single, securely hosted central repository for e-discovery materials with tight security protocols on all paths of access,
- Ensure that e-discovery materials are encrypted at all times, not only when in transit,
- Confirm that cloud services and other vendors use appropriate security measures, and
- Obtain protective orders requiring encryption, access restrictions, access logs and similar safeguards to shield confidential information.

Some clients already have strong cybersecurity safeguards, and they may be reluctant to share electronic data. In such cases, consider storing this information on the client's servers instead.

A new reality

Cyberattacks are increasingly common, and hackers are adept at finding clever new ways to exploit IT systems. So, it's probably not a matter of *if* your firm will be targeted but *when*. CPA experts implement safeguards to prevent cyberattacks and protect critical information from those attackers who manage to get through. Let's discuss how you can implement similar controls to protect clients' electronic data. ■