THOMPSON HINE

Business Law Update

Winter 2014

Distressed Businesses

Good Deals No Longer "Fraudulent" – But May Still Be "Voidable"

Uniform Fraudulent Transfer Act Now Called Uniform Voidable Transactions Act

By Louis F. Solimine

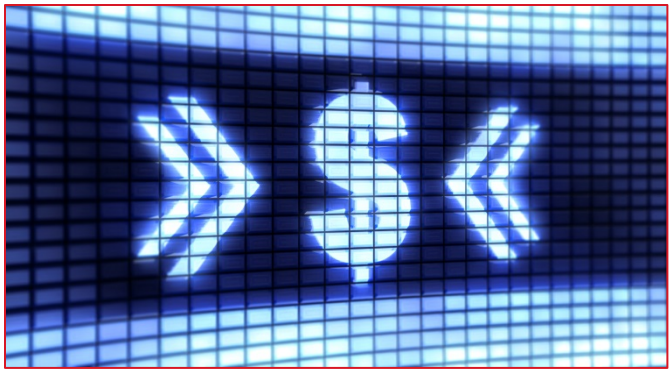
It long has been the law that unpaid creditors of an insolvent debtor can complain if the debtor sells or otherwise transfers any of its assets for less than their fair value. Assume, for example, a company in financial distress sells one of its manufacturing plants to an unrelated purchaser for $15 million. If an unpaid creditor of the seller can demonstrate the fair value of the facility at the time of the sale was $20 million, the purchaser may be required to account to the seller, or its creditors, for the $5 million difference. Similarly, an individual may personally guarantee certain bank loans made to his business. If that business begins to flounder, the individual may be tempted to put some of his assets beyond the reach of his creditors by transferring them to one or more of his family members (or to trusts for their benefit).

These sorts of transactions, where the seller disposes of an asset for less than its fair value, are commonly described in the law as "fraudulent" conveyances. The origins of that term are unclear but it goes back to the Statute of Elizabeth in 16th century England and has been used in the United States for at least nearly 100 years, dating back to the adoption in 1918 of the Uniform Fraudulent Conveyance Act by the National Conference of Commissioners on Uniform State Laws. The Commissioners continued to use the term "fraudulent" in 1984 when they revised the Act and renamed it the Uniform Fraudulent Transfer Act. That same pejorative also has been used for decades in federal legislation such as the Bankruptcy Act of 1938 and its successor, the Bankruptcy Code of 1978 (e.g., 11 U.S.C. § 548 "Fraudulent transfers and obligations").

Recent News & Related Articles

- Potential Changes to OSHA's PSM Standard & EPA's RMP Regulation
- Ohio Supreme Court Holds Borrowers Cannot Raise Standing Challenges in Post Judgment Motions
- SEC Takes Action Against Corporate Insiders for Disclosure Violations
- CFTC Harmonizes General Solicitation Rules With the JOBS Act
- Be Careful What you Wish for: Government Contracting & the Unwary Contractor - Part II
- Be Careful What You Wish For: Government Contracting & the Unwary Contractor – Part I
- Comparing Signature Authority in the U.S. and Germany

For more details on any of the topics covered in this *Business Law Update*, please contact the authors via the links at the end of each article or David R. Valz, editor-in-chief. For information on our Corporate Transactions & Securities practice, please contact Frank D. Chaiken, practice group leader.



The use of the word "fraudulent" has always been a misnomer. Although transfers for less than fair value can be made with an intent to defraud creditors, that is not necessarily the case. In fact, a bona fide, upstanding purchaser which openly and honestly makes a "good deal" to buy a business in financial trouble is not engaged in any fraud at all. To the contrary, the purchaser is only taking advantage of a legitimate business opportunity. Nonetheless, that purchaser still is at some risk that its good faith will be called into question and that it will be forced to account to the seller's unpaid creditors if the price is demonstrably less than the fair value of the purchased assets. And, until now, the purchaser also could be accused of engaging in a "fraudulent" transaction – with all the negative connotations and potential repercussions that entails – even if no fraud has been committed. And, aggrieved creditors may mistakenly have thought they must prove fraud has occurred, even though that is not required.

Finally, this past July, the Commissioners decided to eliminate the word "fraudulent" from the model act and to change its name to the "Uniform Voidable Transactions Act." At the same time, the Commissioners also adopted some relatively minor and technical amendments to the Act, including changes that clarify certain presumptions, burdens of proof and standards of proof, that include a new choice of law provision and that provide a purchaser must provide fair value to the seller (and not to some other person or entity).

The change in the name of the Act may appear, on its face, to be merely cosmetic. However, it is a welcome change which, among other things, will eliminate the stigma of "fraud" from transactions which nonetheless may be questionable. It also, hopefully, will eliminate some of the confusion in the courts, some of which needlessly have grappled with whether a seller or a purchaser must be guilty of actual fraud, or only constructive fraud, for an aggrieved creditor to successfully challenge a transaction. So, purchasers still may discover to their dismay that a deal which is too good to be true may, in fact, be just that. However, once the states adopt the 2014 amendments to the Act and, hopefully, Congress adopts the same terminology, suspect transactions can be evaluated on an objective basis without the need to pin the badge of fraud on anyone.

If you have questions, please contact Louis F. Solimine.

Thompson Hine received eight national first-tier rankings in these areas:

- Bankruptcy and Creditor Debtor Rights/Insolvency and Reorganization Law
- Commercial Litigation
- Construction Law
- Corporate Law
- Litigation – Construction
- Mass Tort Litigation/Class Actions – Defendants
- Real Estate Law
- Transportation Law

Government Contracts

Be Careful What You Wish For: Government Contracting & the Unwary Contractor – Current Ethics Issues & Obligations, Part III

By Lawrence M. Prosen, Daniel P. Broderick & Christian F. Henel

This article is the final installment of a three-part series about current issues involving ethics and government contracting. Throughout this series, we have emphasized the importance for companies contracting with the federal government – either directly *or indirectly* – to understand that federal laws and regulations may, and often do, apply to their contract or subcontract, imposing rigorous ethical standards and compliance burdens.

In this third and final part of this series, we discuss the Covenant Against Contingent Fees, regulation of organizational conflicts of interest (OCIs) and the debarment and suspension procedures the government uses to remove perceived violators from the federal contracting pool. A more detailed version of this article is available on our website.

If you are interested in being added to the firm's Government Contracts mailing list, please contact Kathleen.Steiss@ThompsonHine.com.

Covenant Against Contingent Fees

In the private, commercial context, it is typically not illegal for contractors with an existing relationship with an owner to "sell" access to other contractors or subcontractors in exchange for a contingent fee. In the government contracting realm, however, these types of arrangements generally are forbidden. This relates to a number of already discussed topics, including the anti-collusion/bid rigging and kickbacks and gratuities elements of ethics. In addition, under what is known as the "Covenant Against Contingent Fees," a contractor is not permitted to pay a contingent fee (e.g., a commission) to any contractor, employee or independent agent in an attempt to obtain a government contract. FAR 3.401 defines a "contingent fee" as "any commission, percentage, brokerage, or other fee that is contingent upon the success that a person or concern has in securing a Government contract." Contracts obtained through contingent fees are generally viewed as being the

result of, or giving the mere appearance of, improper influence, defined as "any influence that induces or tends to induce a Government employee or officer to give consideration or to act regarding a Government contract on any basis other than the merits of the matter." The driving policy reason behind the covenant goes to procurement integrity: the government wants to ensure that contractors are selected based on their technical capabilities, their quality, their responsiveness, and the value they provide and not based on "who knows who" and the influence they may be able to exert.

Accordingly, FAR 3.404 and FAR 52.203-5 require that every contract over the simplified acquisition threshold contain the following FAR 52.203-5 clause and warranty:

> *The Contractor warrants that no person or agency has been employed or retained to solicit or obtain this contract upon an agreement or understanding for a contingent fee, except a bona fide employee or agency. For breach or violation of this warranty, the Government shall have the right to annul this contract without liability or, in its discretion, to deduct from the contract price or consideration, or otherwise recover, the full amount of the contingent fee.*

There are two exceptions for a "bona fide" employee or agency that represent a potentially large, but poorly defined, loophole. As the clause states, a bona fide employee or agency is an agent the contractor relies on to contact the government, but who does not assert any improper influence. This could include an internal sales or business capture person or an outside agency. The case law analyzing whether an employee or agent is bona fide is fact-specific and subjective. Thus, the bona fide exception always presents some risk, and contractors considering engaging in these types of contingent fee arrangements should carefully consider the arrangement's terms with the help of counsel.

Organizational Conflicts of Interest (OCIs)

When an incumbent government contractor or one or more of its employees obtains "insider" information resulting from its performance of a government contract, its relationship with the government can give rise to what is known as an organizational conflict of interest or "OCI." The primary consequence of a conflict of interest is that the conflicted contractor cannot be awarded the contract in which it has a conflict unless it can successfully demonstrate that it can mitigate, neutralize or avoid the conflict.

FAR Section 9.5 addresses OCIs. FAR 9.502 generally states that "an organizational conflict of interest may result when factors create an actual or potential conflict of interest on an instant contract, or when the nature of the work to be performed on the instant contract creates an actual or potential conflict of interest on a future acquisition." Courts and boards generally recognize three types of OCIs:

1) **"Biased ground rules,"** wherein a contractor performing a government contract is involved in preparing the rules or requirements for winning a future contract, resulting in its being able to "skew" those rules and requirements in its favor (e.g., performs the design for an item or project to be later procured separately);

2) **"Unequal information,"** where a government contractor gains access to information not known to competitors that it can use to its advantage to win a future contract; or

3) **"Impaired objectivity,"** where a government contractor performing auditing, oversight or similar evaluative services would have the opportunity to evaluate itself, resulting in the natural inference of bias.

FAR 9.505-1 through 9.505-4 provide a series of rules where an OCI **must** result in some restriction on the contractor's procurement eligibility – these are more or less consistent with the three types of OCIs. In addition, FAR 9.508 provides "examples" that illustrate situations where an OCI "may arise." These examples are **not** all-inclusive, but are intended to serve as guidance to contracting officers and contractors. The FAR also requires that contracting officers who anticipate a potential OCI include a provision in the solicitation that identifies the OCI concern and invites offerors to submit an OCI mitigation plan that explains what the offeror will do to neutralize, avoid, or mitigate the conflict (FAR 9.507-1). For a contractor whose conduct may implicate one or more common conflicts of interests, a robust and carefully tailored OCI mitigation plan can be invaluable in allowing that contractor to pursue future government work. Likewise, an insufficient OCI mitigation plan can cost a contractor valuable contracting opportunities.

Suspension and Debarment

The government has the ability to suspend or debar government contractors who violate their legal or ethical obligations. These remedies, which, while tied to the False Claims Act, are administrative and also stand alone, can make the affected contractor – or subcontractor – ineligible to bid on or win future government contracts for protracted periods of time. To avoid debarment, the burden is on the contractor to demonstrate to the debarring official of its present responsibility and that debarment is not necessary (FAR 9.406-1(c)). The decision to debar a contractor must be established by a "preponderance of the evidence" (FAR 9.406-3(d)(3)).

FAR 9.406-2 contains a long list of potential causes for debarment, including: conviction of or civil judgment for committing fraud or another criminal offense in connection with attempting or performing a government contract; violating the Federal False Claims Act; or the catch-all: "commission of any other offense indicating a lack of business integrity or business dishonesty that seriously and directly affects the present responsibility of a government

contractor or subcontractor." In addition, FAR 9.406(b)(vi) states that a contractor can be suspended or debarred if it fails to comply with the mandatory disclosure requirement at FAR 2.1003 that we discussed in Part I of this series. Thus, even if a contractor or subcontractor is not directly liable for violating a law or regulation, it can be penalized for failing to disclose credible evidence of another party's violation in connection with the contract it is performing.

Most debarment decisions are not mandated by law but left to the discretion of the given agency's Suspension and Debarment official. The government's stated policy is to avoid suspending or debarring federal contractors when possible and to do so only in cases where necessary in the public interest; see FAR 9.402: "The serious nature of debarment and suspension requires that these sanctions be imposed only in the public interest for the Government's protection and not for purposes of punishment." That being said, the risk of suspension and debarment can present a serious and potentially devastating reality for contractors even if they ultimately are not convicted of any crime or civil judgment.

Conclusion

The opportunities that government contracts bring to the contractor community are often high-profile, engaging and valuable. Contractors and subcontractors who decide to enter this world can expect to reap many benefits from their relationship with the government but also must be wary of the heightened standards and potential pitfalls that come with their role as a government contractor. We hope this series has been helpful and we look forward to speaking with contractors and subcontractors as needed to help them attain their business goals while mitigating their risk.

This article should not be construed as legal advice. For more information, contact Lawrence M. Prosen, Daniel P. Broderick or Christian F. Henel.

Thompson Hine LLP is pleased to announce its inclusion in the 2014 edition of The Legal 500 United States, a directory of client- and peer-recommended firms, practices and lawyers used by clients throughout the country to guide their selection of lawyers and law firms. Published for more than 20 years, the Legal 500 series provides information and opinions about firms and lawyers across the globe based on interviews with lawyers and representatives from client companies.

In addition, the publication's "Leading Lawyers" listings, which recognize outstanding lawyers nationwide in each practice category, hail Construction practice chair Jeffrey R. Appelbaum as one of the top 22 construction lawyers nationally, and Frank D. Chaiken, chair of the firm's Corporate practice, as one of the country's 23 leading lawyers for middle-market M&A work.

The firm's Corporate Restructuring practice is recommended for providing "a very high level of client service" and for going "above and beyond to assist the client."

Clients commenting on the firm's middle-market M&A practice say its "level of service is excellent. The practice always responds in a timely fashion, provides excellent value, is well versed in industry-specific issues and provides solid and practical advice." Practice group leader Frank Chaiken is singled out for being a "very tactful negotiator."

The firm's Real Estate practice is cited for its successful completion of a wide variety of transactions in 2013, including property acquisitions and development deals. Clients advise that the 15-partner team is "focused and extremely responsive" and has an "incredibly strong" acquisition and development practice. Partner Robyn Minter Smyers is deemed "outstanding."

Public Companies

Private Stock Repurchases: What to Look Out For

by Jurgita Ashley

Say an executive officer or a member of a public company board is retiring and would like to sell his or her shares back to the company. Or perhaps an investor wants out of the stock, but faces practical issues with disposing of a large block of stock on the open market due to limited liquidity in the company's stock. Assuming the company is willing to facilitate a repurchase, when and how is it permissible for the company to repurchase the stock in a private transaction?

In most cases, privately negotiated repurchases can be completed relatively quickly and can be an effective way for a public company to manage insider dispositions.

In many cases, a privately negotiated repurchase can be effected in short order. As officers of a company do not have inherent authority to repurchase company stock, a board authorization covering the private repurchase needs to be in place; this can be covered within the scope of resolutions authorizing a stock repurchase program. The board should remain mindful of its fiduciary duties and state law limitations on repurchases, which generally require repurchases to be paid out of surplus (i.e., the excess of the company's net assets over the par value of the company's issued and outstanding common stock) and not to impair the company's solvency (e.g., the ability to pay debts as they come due). If the shares are being repurchased from a member of the board or an investor who has a representative on the board, and board approval needs to be sought for that particular repurchase due to fiduciary duty and conflict of interest considerations, such board member or investor representative should abstain from voting on the matter. If there are any concerns regarding Section 16(b) profit-disgorgement issues for the insider selling the shares, the particular repurchase may also need to be approved specifically for Section 16 purposes by a compensation committee comprised solely of non-employee directors, or the six-month periods on either side of the repurchase may need to be carefully monitored for potential matching opposite-way transactions.

The repurchase terms can be documented in a simple agreement. The agreement should specify the purchase price, purchase time and the method of transferring the shares. Repurchases are typically effected either at the market price or at a discount – at times a significant discount – to the market price as the company is providing liquidity to the investor, which may otherwise be significantly limited. In any case, the company should ensure that the seller has a clear, unencumbered title to the shares, and at a minimum both parties should provide representations regarding their authority and necessary authorizations to enter into the repurchase agreement and to effect the transaction.

A single or a few isolated private repurchases do not trigger tender offer concerns, and private repurchases do not impact the company's public repurchase program under Exchange Act Rule 10b-18. If there are multiple private repurchases, companies should ensure that each is separately negotiated and not part of a larger repurchase program to avoid aggregation of company purchases and, consequently, creeping tender offer issues. "Going-private" rules should also be kept in mind, but are generally unlikely to be triggered by isolated private repurchases.

General anti-fraud and market anti-manipulation considerations apply to private repurchases, which are heightened if the company is contemplating a strategic

transaction or a securities offering. Neither the company nor the seller should be trading on the basis of material non-public information. Although, in general, the company has the same information as the retiring board member or executive, or an investor with representation on the company's board, the repurchase agreement should be entered into, and the repurchase should be effected, in compliance with the company's insider trading policy and, preferably, during an open trading window (i.e., outside of either a regular or special trading blackout).

Privately negotiated repurchases trigger minimal public disclosure obligations for the company. The company is required to report all repurchases in its quarterly report on Form 10-Q or annual report on Form 10-K. A repurchase in excess of $120,000 from a current insider or a greater-than-five percent beneficial owner could trigger a related party disclosure in the company's proxy statement, and a significant repurchase may also require a current report on Form 8-K, including the filing of the repurchase agreement as an exhibit to the company's SEC filings. Certain repurchases may also trigger notifications to a stock exchange. For the seller, repurchases by the company are not subject to volume limitations under Securities Act Rule 144, but may require a filing of a beneficial ownership report on a Form 4 and/or an amendment to the investor's Schedule 13D/G.

Although they are not widespread and only limited in application, state anti-greenmail statutes should also be considered. Selling shareholders should also consider the potential applicability of anti-greenmail provisions in the U.S. tax code, and parties should keep in mind state "interested shareholder" statutes. Companies may also have anti-greenmail or other provisions in their certificate of incorporation or bylaws that could prevent repurchases. The company should also review its credit and other material agreements to ensure that any repurchase is within the permitted scope.

While the foregoing considerations should be kept in mind, in most cases privately negotiated repurchases can be completed relatively quickly and can be an effective way for the public company to manage insider dispositions.

For more information, please contact Jurgita Ashley.

Cybersecurity

Despite Lack of Regulatory Guidance, Companies (and Their Executives) Need to Protect Themselves

By James M. Roberts

Did you know that October was National Cybersecurity Awareness Month? President Obama issued a proclamation at the end of September 2014 calling for activities, events and training in observance of the importance of cybersecurity. By now, of course, no businessperson needs a presidential proclamation to know that addressing cybersecurity is critical to the survival and success of any organization. Senior management and boards of directors need to be asking themselves and their organizations important questions like "What is the liability? How do we protect ourselves – not just from attack, but from regulators and shareholder litigation – if, and when, an attack is successful?" If for no other reason, the imposition of individual liability on officers and directors for their company's data security incidents should encourage a tight focus on data protection.

Recent high-profile data breaches demonstrate that cybersecurity is no longer a technical issue to be relegated to an organization's information technology group. Companies' data security is now a topic that demands attention and direction from the C-suite, as well as the board of directors. The Target and Home Depot data breaches have shown that in addition to the reputational and brand consequences of a data breach and follow-on government enforcement and class-action lawsuits, directors and officers of companies now are exposed to potential shareholder litigation for failing to implement and maintain adequate measures to protect company, employee and customer data, and thus, the theory goes, breaching their duty of oversight, care and loyalty.

Clear, uniform federal guidelines expressing what steps companies need to take to protect information and notify authorities or individuals of a breach do not appear to be forthcoming. During congressional hearings held to investigate the Target breach, some congressional representatives expressed concern about the absence of such guidance. Others noted that imposing such standards that may be outpaced by innovation would impose unnecessary expense on companies. Although a current draft bill, the Cybersecurity Information Sharing Act, seeks to harmonize the process for sharing information about security measures and attacks, similar versions of the bill have failed to pass the Congress four times. Commentators generally agree that any clear guidance emanating from the current Congress is unlikely.

In the absence of clear legislative guidance, what is a corporation to do? At the federal level, actions against companies initiated by the Federal Trade Commission have provided one source of information. Over the past 12 years, the FTC has commenced 50 actions against companies that failed to implement effective cybersecurity measures resulting in what it alleges are "unfair practices." The FTC has also asserted jurisdiction when it determines that a company is not following its own cybersecurity protocols under a theory that that is tantamount to engaging in "deceptive trade practices." State attorneys general similarly have enforced their states' own consumer protection and data security laws in response to significant data breaches.

Most of these actions, such as the one against Fandango, result in multi-decade final orders that prohibit the company from "misrepresenting the extent to which they maintain the privacy and security of consumers' personal information." In addition, the companies must adopt comprehensive security programs to protect consumers'

personal information. These programs are usually subject to evaluation by external third parties. These orders use fairly standard language and require that the company in question:

1) Designate an employee or employees to coordinate and be accountable for information security;

2) Identify material internal and external risks to personal information and assess the safeguards to control those risks;

3) Regularly test those safeguards;

4) Develop and use reasonable steps to select and train service providers (vendors); and

5) Evaluate and adjust the safeguards based on the risk assessments, material changes to business arrangements, or any other facts that the company knows or has reason to know might materially impact the effectiveness of the security program.

Such dictates are not the stuff of regulatory transparency.

In January of this year the SEC waded into the fray, announcing that technology and cybersecurity were examination priorities. In April, the SEC issued a Risk Alert announcing that it would examine over 50 companies' cybersecurity protocols. The alert appended a standard document request relating to cybersecurity addressing six topics: identification of risks/cybersecurity governance; protection of firm networks and information; risks associated with remote customer access and funds transfer requests; risks associated with vendors and other third parties; detection of unauthorized activity; and, other (including reporting security issues to regulators and law enforcement, identifying identity theft red flags, identifying security best practices, etc.). Although one can reverse-engineer some necessities (e.g., adopting risk management standards such as those issued by the National Institute of Standards and Technology and the International Organization for Standardization), it is unclear what happens if, say, a company fails to have a Chief Information Security Officer.

If you're doing business in California, you may have already considered that your company will have to take steps this year to secure your data. At the end of September, California passed legislation which again altered its cybersecurity statute. In the most recent iteration, it requires that companies that retain personal identifying information implement and maintain "reasonable security procedures and practices" to protect personal information from unauthorized access, destruction, use, modification or disclosure. Notably, this bill, like its federal counterpart, had stronger language about companies' encryption and notification requirements in the original draft, but those specifications were stripped from the final bill. In the absence of standards, though, companies may find themselves having to convince the Attorney General of California that their measures were eminently reasonable. In addition, companies that choose to offer identity theft prevention and mitigation services after a breach must offer it to customers for free and for no less than 12 months. Similar legislative obligations are the law in Massachusetts and Nevada.

Companies must prioritize cybersecurity; of that there is little doubt. What is unclear is precisely what steps need to be taken in order to not only protect your organization from a breach, but also protect it from civil and regulatory liability. Although imposition of standards across industry may be costly and onerous, the vacuum that is created in the absence of legislation may be filled by state attorneys general that have different views of what is reasonable and what is not reasonable. As a result, companies and executives can find themselves in the roles of both victim and target and need to take into account both roles in identifying ways to protect their customers and themselves.

To learn more, please contact any of the professionals in our Privacy & Information Security practice group.

Corporate Governance

The Battle Over Fee-Shifting Bylaws

By David J. Willbrand & Emma Scharfenberger Off

The ruling by the Delaware Supreme Court in *ATP Tour, Inc. v. Deutscher Tennis Bund* made on May 28, 2014 opened the door for Delaware corporations to adopt fee-shifting bylaws or charter provisions to recover expenses, including legal fees, incurred by the defending corporation as well as its officers, directors, and/or their affiliates and all other defendants against a stockholder pursuing intra-corporation litigation if the stockholder is unsuccessful in the litigation or arbitration. Since then, 24 companies have adopted either a fee-shifting bylaw or charter provision, including Alibaba Group Holding Ltd. (Alibaba) before it went public in September.

ATP Tour Inc. v. Deutscher Tennis Bund

In *ATP,* the Delaware Supreme Court provided an *en banc* opinion to a certified question of law asking whether ATP Tour, Inc.'s fee-shifting bylaw was valid and enforceable under Delaware law. The Court upheld the facial validity of the fee-shifting bylaw. In reaching its decision, the Court reasoned that fee-shifting bylaws are not prohibited under the Delaware General Corporation Law (DGCL), any other Delaware statute, or Delaware common law. The bylaw was held to be facially valid for this reason and because it did not conflict with the corporation's certificate of incorporation. However, the Court reminded that even a facially valid bylaw will not be enforced if it's adopted or used for an inequitable purpose. Intent to deter litigation is not invariably an improper purpose in the eyes of the Court. Though ATP Tour, Inc. is a non-stock corporation, the Court's reliance on general corporate law principles and the DGCL suggests its decision also applies to stock corporations. The Court did not address the specific merits of the bylaw at issue in *ATP.*

The *ATP* Aftermath

In the wake of this decision, the Delaware Corporate Law Council proposed statutory amendments to nullify *ATP's* holding with respect to stock corporations. Senate Bill 236 was proposed on a fast track to the Delaware General Assembly but was never put to a vote due to questions that arose during the legislative process. Instead, Senate Joint Resolution #12 was adopted by the Delaware legislature, signed by the Governor and became law on June 30, 2014. This Resolution calls for continued examination of the proposed anti-fee-shifting amendment embodied in Senate Bill 236 prior to the commencement of the next legislative session in January 2015.

Interestingly, the Investor Advisory Committee of the Securities and Exchange Commission (SEC) took the issue of fee-shifting bylaws up at its October 9, 2014 meeting. Professor John C. Coffee, Jr. of Columbia Law School, who testified before the Committee, characterized the *ATP* decision as "the first trickle through a leak in the dam" that eventually causes the dam to collapse. It is unclear what role the SEC will play in the fee-shifting debate or what action the SEC will take against corporations who include fee-shifting provisions in their registration statements. The SEC did not take action against Alibaba, which included such provision in its registration statement.

Finally, the Oklahoma legislature has adopted a bill allowing for a variation of fee-shifting bylaws. In Oklahoma, the nonprevailing party in a shareholder derivative action must pay the prevailing party the reasonable expenses, including legal fees, incurred as a result of such action. This variation is narrower than the bylaw held to be facially valid by the Delaware Supreme Court because it applies only to derivative suits. Additionally, it is more equitable, as it

provides for the awarding of expenses for the successful derivative plaintiff (not just the successful corporation).

Continued Adoption of Fee-Shifting Bylaws

Though only 24 public companies have adopted fee-shifting bylaws or charter provisions since May, the adoption rate continues to grow. At the moment, private and public companies incorporated in Delaware should consider adopting fee-shifting provisions (although companies which are currently embroiled in stockholder litigation may wish to wait, as adopting provisions of this sort within that context may be perceived as inappropriate and in bad faith). That being said, careful monitoring of the Delaware courts and legislature, as well as the SEC, would be advised, as the last chapter has yet to be written, and subsequent actions may necessitate a company's modification or even outright elimination of fee-shifting provisions.

To learn more, please contact David J. Willbrand or Emma Scharfenberger Off.

Thompson Hine LLP has been recognized for the eighth consecutive year as being among the top 30 firms nationally for excellent client service in the BTI Client Service 30. The firm placed fifth in the nation for overall client service, marking the firm's third year in the top 10. The firm scored in the top four nationwide for "Provides Value for the Dollar" and "Commitment to Help."

Thompson Hine has also been named to the BTI Client Service A-Team, of which the Client Service 30 is a subset, for 14 consecutive years (since the survey's inception).

"Thompson Hine again is recognized for its superior performance in our 14th annual general counsel surveys. Ranked overall among the top five firms in the country for client service, as well as in the top four firms nationwide for the two areas identified as the most important to clients – providing value and commitment to help – Thompson Hine has appeared on the BTI Client Service A-Team in every year since the inception of the survey," says BTI President Michael Rynowecer. "Thompson Hine's longtime focus on client service and continuing focus on aligning to respond to a changing market drives high marks from a client base eager for greater value from their law firms."

Thompson Hine receives this recognition at a time when clients are seeking significant changes in the way legal services are delivered. The firm, which is heavily invested in and committed at its highest levels to innovate its service delivery, has responded by changing its service delivery model through its innovative SmartPaTH℠ initiative, adding personnel, software, infrastructure and practice management in areas including process efficiency, legal project management, value-based pricing and flexible staffing.

"Thompson Hine remains committed to providing our clients high value and excellent service. We have been shifting the focus of our service delivery to address our clients' needs for predictability, efficiency and transparency, which yields greater value and offers better solutions. We continue to invest in innovations to enhance the way we manage our legal services," said Deborah Z. Read, the firm's managing partner. "Our priority is refining our model to align our service delivery with our clients' business goals."

The BTI Client Service 30 represents the cream of the crop of the BTI Client Service A-Team. BTI's exclusive research reveals that large and Fortune 1000 clients nominated 337 core law firms for superior client service this year – and a mere 30 distinguish themselves as the absolute best, outperforming their peers by a factor of 6. BTI scores firms based solely on unprompted feedback from over 300 corporate counsel, using a client-driven ranking of the importance and influence of each of 17 client service activities. Law firms in the BTI Client Service 30 have truly differentiated themselves in the eyes of clients.

Directors: Do Your Homework, Even if You Get it Wrong

A Review of the Recent Georgia Supreme Court Decision Construing the Business Judgment Rule

By Michael V. Coleman and Tara N. Evans

Introduction

The business judgment rule has been relied upon for decades by directors of corporations to protect them from liability. The business judgment rule provides that directors will not be liable for decisions that they make, so long as they employ the basic tenants of their fiduciary duty – good faith, loyalty and due care – in their decision making. While the business judgment rule has been the subject of extensive litigation over the years, it had never been directly addressed by the Supreme Court of Georgia until its July 2014 decision in *FDIC v. Loudermilk*.[1]

In its first direct discussion of the business judgment rule, the Court firmly cemented the doctrine in Georgia jurisprudence. The Court determined that the business judgment rule protects directors of Georgia corporations from liability for the merits of decisions that they make, so long as they (i) conduct adequate due diligence, (ii) engage in appropriate deliberation, and (iii) do not act in bad faith. The Court rejected the notion asserted by the defendants that the business judgment rule provided blanket protection for **all** negligence claims against directors. While directors cannot be liable for bad decisions, they can be liable for such decisions if they do not follow an appropriate deliberative process.

The Loudermilk Decision

The Loudermilk decision arose out of a case in which the Federal Deposit Insurance Corporation (FDIC), as receiver for the Buckhead Community Bank, sued nine former officers and directors of the bank for certain loans which resulted in a $22 million loss to the bank. Although the case involved the alleged negligence of bank directors, the ruling regarding the business judgment rule applies to directors of all Georgia corporations.

The Court first concluded that the business judgment rule was a settled part of Georgia common law, and that it would generally preclude claims based on ordinary negligence, "except to the extent that those decisions are shown to have been made without deliberation, without the requisite diligence to ascertain and assess the facts and circumstances upon which the decisions are based, or in bad faith."[2] In other words, directors cannot be liable for the substance of their decision, unless they were negligent in **the process** of making the decision. If the process is diligent, deliberative and in good faith, the Georgia courts will not question the substance of a decision that turns out to be wrong.

Having firmly established the business judgment rule as part of Georgia corporate law, the Court then determined that the rule was consistent with the Banking Code. Specifically, the Court ruled that the "ordinary diligence, care and skill" referenced in O.C.G.A. § 7-1-490(a) (describing the standard of care for bank officers and directors) pertains to "ordinary diligence, care and skill" with respect to **the process** of making the decision, rather than the substance of the decision. Notably, the Court stated that the Banking Code specifically provided that it was reasonable for bank directors to rely on reports from others in their decisions.

Practical Considerations

Here are a few pointers which should help protect directors from potential liability. Directors should:

- Participate actively in board meetings.

[1] *FDIC v. Loudermilk*, 295 Ga. 579 (2014).

[2] *Id*. at 585.

- Review all information presented in connection with potential decisions.
- Ask questions and request additional information that might be helpful.
- Ask for reports or summaries regarding any aspect of a decision (particularly bank directors).
- Feel free to rely on reports from accountants, attorneys or other experts.
- Ensure that the record reflects a thorough discussion of the various issues.
- Make decisions that they believe to be in the company's best interests.
- State the reasons why they believe their decision to be in the company's best interests.

If a director follows these steps, he or she is likely to be protected from liability by the business judgment rule, even if a decision turns out to be wrong.

For more information, please contact Michael V. Coleman or Tara N. Evans.