The Polsinelli Pulse

MITIGATING LITIGATION RISK AT THE DEAL TABLE AND BEYOND

NEWSLETTER FROM THE M&A LITIGATION PRACTICE

Mergers & Acquisitions and Paycheck Protection Program: Proceed with Caution

Philip G. Feigen
Office Managing Partner
Washington, D.C.

Sara C. Ainsworth
Associate

In Spring 2020, Congress adopted the CARES Act, which authorized $350 billion for the Paycheck Protection Program ("PPP"). With an additional $310 billion authorized under the PPP Flexibility Act in June 2020, PPP ultimately provided $660 billion for guaranteed loans to U.S. small businesses experiencing significant financial problems due to the Covid-19 pandemic.

The U.S. Small Business Administration ("SBA") and the U.S. Department of Treasury ("Treasury") are tasked with implementing and overseeing the PPP, including issuing regulations and interpretations. Additionally, in December 2020 Congress passed the Economic Aid Act, which provided an additional $284 billion for the creation of second draws from the PPP ("PPP2"). The SBA and Treasury are now issuing additional regulations and interpretations related to PPP2 and implementing changes to PPP as outlined in the Economic Aid Act.

In the rush to create PPP, the consequences of certain business transactions were not fully considered. While SBA and Treasury issued guidance related to changes of ownership in the initial round of PPP, the agencies have yet to issue guidance related to the intricate issues surrounding PPP2. These issues range from the eligibility of entities for additional PPP loans after the acquisition of a business that held a PPP loan to navigating merger transactions between parties that both have PPP loans. This article addresses tips for those businesses that are contemplating such transactions, whether or not the PPP loan was entirely forgiven, partially forgiven or remains outstanding.

Due Diligence

The PPP issue must be addressed during due diligence. An acquirer should request a target's original PPP application, the PPP loan (and any associated documentation) issued from the PPP lender, the forgiveness application (if completed or available), and, if available, evidence of SBA approval of forgiveness and/or a bank payout letter. In addition, if the target is a larger borrower, with a PPP loan of over $2 million, a copy of the necessity questionnaire (if filed).

Why are these documents important? To the extent the PPP loan had been paid off, an acquirer needs to ensure that it has been done properly. If the loan is still outstanding, the acquirer will want to ensure that the funds have been used properly (as evidenced by the forgiveness application) and determine whether the transaction will require the bank and/or SBA's approval.

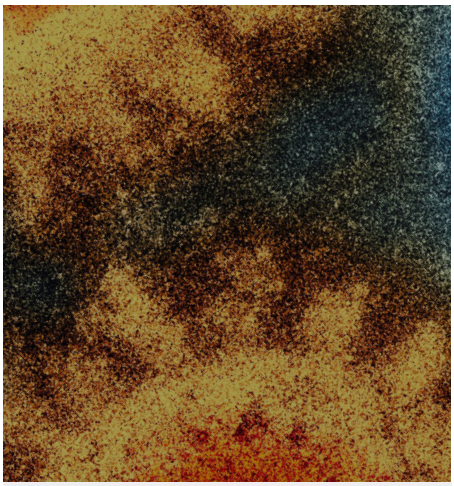
> *Particularly regarding an equity transaction, it is important to ensure that the acquirer has all of the necessary documentation, as the SBA may audit a PPP borrower for up to six years after receipt of the loan.*

Further, depending on the structure of the transaction, there may be concerns about successor liability.

CONTINUED ON PAGE 2

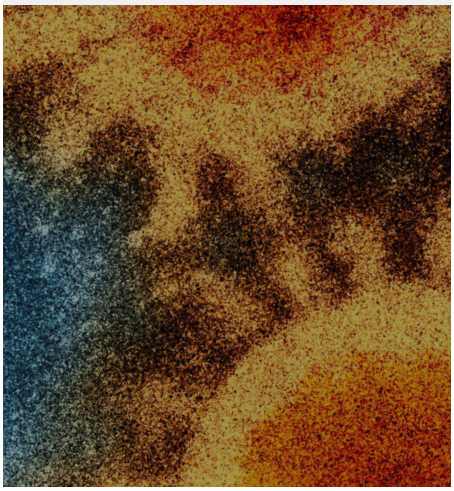
CONTINUED FROM PAGE 1

Table of Contents



COVID-19: What Your Business Needs To Know

Click **here** to join our mailing list and receive new blog posts, event information and COVID-19 legal updates direct to your email inbox.



Change of Ownership

What transactions require SBA approval, SBA notification or use of a potential safe-harbor? The SBA issued guidance on October 2, 2020 (the "Guidance"), which set forth how to handle changes of ownership when a borrower has an outstanding PPP loan. The Guidance defines changes of ownership as:

- The sale or transfer of 20% of the common stock or other ownership interest of a PPP borrower.
- The sale or transfer of at least 50% of a PPP borrower's assets (as measured by fair market value).
- The merger of a PPP borrower with or into another entity.

It's important to note that all sales and transfers since the date of approval of the PPP loan have to be aggregated to determine whether the above threshold has been met.

For an equity transaction, SBA approval is not required if the sale of equity is for 50% or less of the PPP borrower's equity. Further, SBA approval will not be required for any other change of ownership — merger, sale of 51% or more of equity or sale of 50%+ of assets — if the PPP borrower (1) applies for forgiveness and (2) escrows the full amount of the PPP loan in an escrow account controlled by the PPP lender. With respect to timing, it is important to note that the forgiveness application and escrow need to be completed *prior* to the closing of the transaction. The escrow will then be released upon the SBA's decision regarding forgiveness.

If a PPP borrower cannot either apply for forgiveness or escrow the funds, SBA approval is required, which can take months to process. In addition to the above requirements, any sale of equity or merger requires notice to the SBA of the new owners of the PPP borrower.

For transactions in which both parties have PPP loans, the new owner or successor will be responsible for segregating and delineating PPP funds, expenses and documentation. In such a scenario, it is very important for both the target and acquirer to have their documentation in order before closing the transaction.

The SBA is not the only party whose approval may be necessary in a change in ownership. Depending on the structure of the transaction and the terms of the PPP loan document, lender consent may be necessary as the transaction may be concerned with an event of default. It is important to discuss the transaction with the lender early on, as they may need to be intimately involved, whether to liaise with the SBA, provide the escrow account or give consent.

PPP2 Nuances

The creation of the PPP2 creates several interesting situations. Under PPP2, a borrower can only get a second draw PPP loan if it previously received a PPP loan. Additionally, the Economic Aid Act reopened the first round of PPP loans for eligible borrowers that did not receive a PPP loan in the first round. This creates the following unresolved scenarios:

- Is a company that never received a PPP loan but acquired a company with a PPP loan:
  - Eligible for PPP2?
  - Eligible for an initial PPP loan?
  - Not eligible for any additional PPP loans?

Unfortunately, there is no clear answer to any of these scenarios. In the first scenario, it is unlikely that the company would be eligible for PPP2 as the SBA would not have documentation of the initial PPP loan. In the second scenario, this would seem like double-dipping and likely would not be allowed. The third scenario seems like somewhat of an illogical result if the company is otherwise eligible for PPP. Unfortunately, without further guidance from the SBA it is not clear how to proceed in these scenarios.

Conclusion

Proceeding with an M&A transaction when a PPP loan is involved requires advance planning. Once you have fleshed out the issues in due diligence, it is important to discuss the situation with the PPP lender to navigate consent. Not all lenders are familiar with the change of ownership rules, so counsel can assist in educating the PPP lender to avoid any last-minute issues.

Cyber Comes to the C-Suite: New D&O Exposures in the Aftermath of *First American*

John C. Cleary
Shareholder

Alexander D. Boyd
Associate

Cyber risk comes in all shapes and sizes and never really stands still. The cyber threat environment continually brings new attack methodologies while the legal and enforcement environment brings ever-growing legal obligations, express or implied, to safeguard networks and the information residing on them.

The C-Suite, sitting atop our largest organizations, has long been aware of these characteristics of cyber risk and increasingly finds itself tasked by law (or lawsuits) with understanding and managing them as a competitive and legal necessity. Nowhere is this more acutely seen and demonstrated in recent months than by the ongoing travails of First American Financial Corporation, a strong and reputable Fortune 500 company whose leadership now faces potential civil liability in Delaware for alleged mismanagement of cyber risk, lack of controls and flawed communications and disclosures about cyber risk and adverse cyber events.

The case, filed on November 25, 2020, is a shareholder derivative suit against First American and certain of its officers and directors in federal court in Delaware (*Hollett v. Gilmore, et al.*, No. 1:20-cv-01620 (D. Del. 2020). Capping an 18-month cyber odyssey for the company, it opens a window into the internal governance and oversight challenges posed by cybersecurity risk, both for companies in the ordinary course and companies buying or selling other companies. Our purpose here is to peer into that window and to identify challenges facing directors and officers in the management of cyber risks going into the balance of 2021.

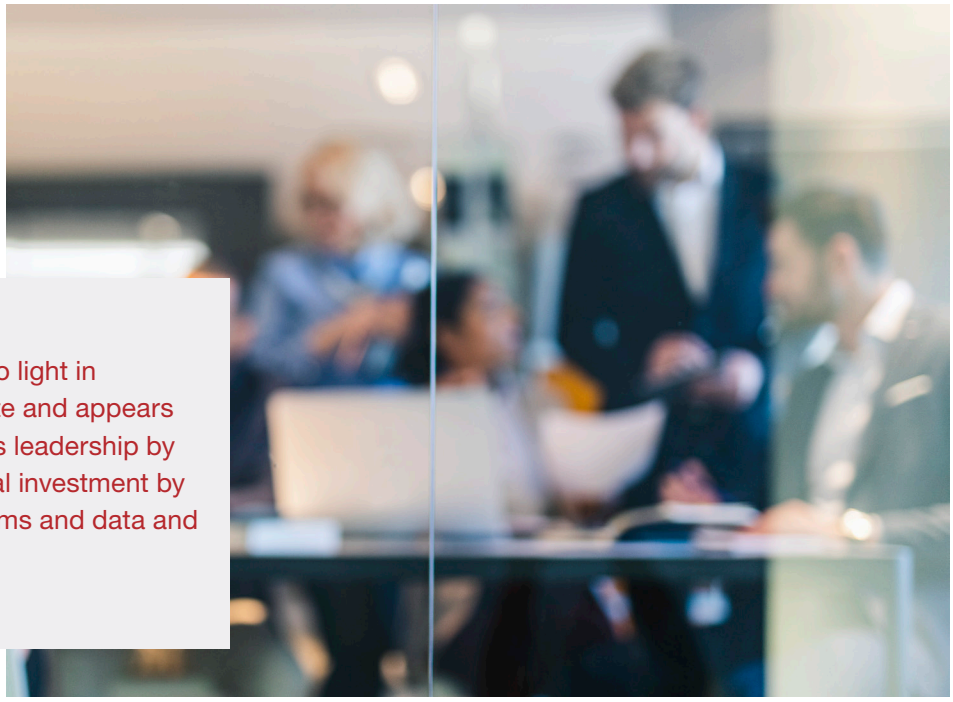
First American is the second-largest title insurance provider in the U.S. with revenue for the fiscal year ended December 31, 2019, totaling approximately $6.2 billion. The company collects sensitive personal information from its customers as a part of the title insurance application process and stores the information in First American's "FAST" document repository. First American also created a web-based platform allowing these documents to be shared through a uniform resource locator (URL) that would allow customers to access their documents. It turns out that anyone else who had the URL or guessed it by accident or experimentation could also access the documents. First American's data portal first became vulnerable in October 2014. Since that time, more than 850 million FAST documents were potentially exposed.

First American had extensive cybersecurity measures and staffing in place and discovered the vulnerability in December 2018 during a penetration test. However, the company did not begin to address the vulnerability until six months later after a journalist, Brian Krebs, learned of the vulnerability and made it public.

An investigation by the New York Department of Financial Services ("DFS") later suggested that First American's Board was aware of key aspects of this vulnerability as early as April 2018.

New York Department of Financial Services

First American is regulated by DFS, an agency that has been at the forefront of regulatory oversight since 2017 and that has long required "ownership" by the C-Suite of cybersecurity at financial services firms under its jurisdiction. DFS rules and regulations (23 NYCRR Part 500) require annual certifications by company leadership and generally impose more rigorous duties than typically required by common law and even Delaware law. Akin to Sarbanes Oxley



The *First American* incident came to light in May 2019 through the Krebs website and appears to have taken First American and its leadership by surprise notwithstanding substantial investment by the company in protecting its systems and data and managing its cyber risks.

CONTINUED ON PAGE 4

CONTINUED FROM PAGE 3

certification requirements introduced roughly two decades ago, the DFS requirements for companies and their C-Suites (namely the Chief Information Security Officer ("CISO") have considerable specificity and regulatory enforcement "teeth" and, as a practical matter, take these obligations to a new level.

DFS cybersecurity regulations mandate that covered organizations maintain written policies to protect information systems and nonpublic information, limit user access privileges, conduct risk assessments, train employees, and encrypt data in transit and at rest. The regulations require prompt notice to DFS within 72 hours of discovering a cybersecurity event.

DFS regulations also require each covered organization to designate a qualified CISO to implement and enforce the organization's cybersecurity policy. The CISO must provide an annual report to the organization's board of directors. The report must consider and address the organization's cybersecurity program and the risks facing the organizations. Furthermore, and perhaps most importantly, the regulations require an annual written certification of the company's compliance with DFS mandates, signed by either a "Senior Officer" of the company or the "Board of Directors" through the "Chairperson of the Board of Directors."

DFS's Investigation of First American

Notified by First American after the matter had already been made public by the Krebs website, DFS investigated at considerable length, focusing on the underlying forensics issues as well as management and oversight lapses that left the vulnerabilities largely unknown to company leadership and unreported to the company's regulators. On July 21, 2020, DFS issued its detailed factual findings and commenced an enforcement proceeding leveling six "charges" against First American. This was the first enforcement action by DFS under the new regulations and it was chosen to send a message that DFS would be actively enforcing its cybersecurity requirements.

DFS alleged that First American failed to:

- Maintain an adequate cybersecurity program.
- Perform periodic risk assessments for data stored or transmitted within its systems.
- Maintain data governance and classification policies or maintain access controls on its platform.
- Implement reasonable access controls to limit access to personal information.
- Provide adequate data security training for its employees and affiliated title agents.
- Encrypt sensitive documents stored within the FAST repository.

DFS sought unspecified "civil monetary fines against [First American] pursuant to Financial Services Law Section 408" and an order requiring First American to remedy the alleged violations. But an accompanying press release from the New York Attorney General left no doubt where DFS wanted to go with this case:

> *"DFS alleges that each instance of Nonpublic Information encompassed within the charges constitutes a separate violation carrying up to $1,000 in penalties per violation."*

Thus, if taken literally, the face amount of this case as pleaded could be 850 million documents times $1,000 or $850 *billion*. Commentators have differed as to whether this could even be remotely correct or plausible under the language of Section 408, and there is certainly a defensible interpretation that would value the case as six pleaded types of infraction for a $1,000 maximum penalty each, or a total exposure of $6,000. The case has been closely watched and remains pending.

Unlike civil litigants, DFS has no obligation to plead or prove injury to individuals. Indeed, DFS makes no allegation that the 850 million allegedly "exposed" or "compromised" records were accessed, viewed or acquired by unauthorized persons, other than a subgroup of about 350,000 records that may have been compromised in an automated fashion. It is certainly possible that no such injury will ever be found. Nevertheless, injury or no injury, the Krebs article in May 2019 and the DFS findings in July 2020 set the scene for the veritable avalanche of problems that descended on the company:

- An investigation and Wells Notice from the U.S. Securities and Exchange Commission
- A dozen or more data breach class action lawsuits by alleged victims of the incident.
- A securities fraud class action lawsuit in California.

Shareholder Derivative Suit against First American Officers and Directors

A shareholder derivative suit encompassing all of these issues and problems soon followed. Stockholders allege, on behalf of the corporation, that First American officers and directors failed to divulge the "full truth" of the company's cybersecurity issues until its SEC Form 10-Q filing for the Third Quarter of 2020, which First American filed on October 22, 2020. The complaint further contends that officers and directors mismanaged the company's cybersecurity defenses over a sustained period, exaggerated the nature and strength of such defenses, failed to maintain adequate controls and failed to respond with timely and accurate information when a massive breach of such defenses was discovered and publicized by a journalist. The ten individual defendants have been sued for "breaches of their fiduciary duties as directors and/or officers of First American, unjust enrichment, abuse of control, gross mismanagement, waste of corporate assets, violations of Sections 14(a) of the Securities Exchange Act of 1934 (the 'Exchange Act'), and for contribution under Sections 10(b) and 21D of the Exchange Act."

The case is at its earliest stages and will be watched closely from both a cyber-liability perspective and from a director's and officer's liability perspective.

Takeaways and Next Steps

The *First American* incident came to light in May 2019 through the Krebs website and appears to have taken First American and its leadership by surprise notwithstanding substantial investment by the company in protecting its systems and data and managing its cyber risks. The resultant cascade of legal problems, culminating in the latest derivative suit, give rise to some key takeaways for organizations and their leadership:

- **Governance —** Cybersecurity needs to be fully embedded in the organization, with true subject matter ownership and expertise at the C-Suite level, such as a strong CISO, coupled with strong, committed, and competent board oversight. The DFS mandates are a useful and compelling start on these governance measures, but other frameworks can help drive these initiatives as well, such as those sponsored by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), the Center for Internet Security Risk Assessment Method (CIS-RAM), and others. Whether traditionally regulated or nonregulated entities, whether in New York or other states, all organizations must now take these cybersecurity governance issues seriously.

CONTINUED ON PAGE 5

CONTINUED FROM PAGE 4

- **Continuous Improvement —** Cybersecurity needs to be a continuous, "long haul" commitment, facing ever-changing threats and risks and drawing upon the best available industry insight and expertise. No one saw the First American scenario coming, yet it is painfully obvious with the benefit of hindsight.
- **Materiality —** Beware of the so-called "*de minimis*" or "nonexistent" problem. Certainly, a company in First American's situation would prefer to treat an apparent "no-harm-no-foul" incident like this one as a non-event. But, as explained above, that is not the lens through which DFS views these matters in New York, nor courts and regulators elsewhere if present trends continue. Battalions of data breach class action lawyers and securities fraud class action lawyers also seem willing to join this fray. Cyber risk includes risk of injury to individuals, as well as regulatory risk and reputational risk. All must be taken into account in assessing materiality or even in conducting a cost-benefit analysis to justify additional expense and investment in cybersecurity.
- **Ubiquity —** Officers and directors face cyber risk in virtually every direction these days, from everyday operations of a company that needs or utilizes personal information of individuals (like the First American scenarios), to a mergers and acquisitions scenario (as was experienced by Yahoo and others), to generalized brand management, public relations, advertising and communications. The response, in turn, must be comprehensive as well.
- **M&A Due Diligence —** *First American* provides important reminders for organizations conducting due diligence on a potential acquisition: An increasing number of industries and jurisdictions require organizations to implement and enforce comprehensive cybersecurity programs. Failing to adhere to those requirements can create risk at all levels of the organization that could be passed on to a successor. Additionally, even organizations that have sophisticated cybersecurity programs (like First American) can run into trouble if they underestimate or fail to identify suspected vulnerabilities or incidents. Buyers should be careful to examine a target organization's written policies and procedures, records demonstrating adherence to those policies, records related to any audits or tests and the remediation of any deficiencies, and documentation ensuring the organization is complying with all applicable data privacy and cybersecurity laws.

Deal Scrutiny — Standards of Review & Decision Makers in Different Jurisdictions

Robert V. Spake, Jr.
Shareholder

Gordon D. Spring
Shareholder

For M&A practitioners, potential deal scrutiny informs the process by which deals are structured. Understanding the applicable legal standard is a critical first step to determining if directors have complied with their fiduciary duties. This article looks to a potential deal in Delaware (where a judge decides the case on a well-developed body of case law) and outside of Delaware (where often a jury is the ultimate decision-maker and standards of review vary).

Delaware

Delaware is the preeminent state for corporate formation and corporate law. Many deals include Delaware forum selection and choice of law clauses. Even when Delaware law does not govern, many states look to Delaware corporate law for guidance.

Under Delaware law, fiduciaries owe duties of care and loyalty. A court determines whether a fiduciary fulfilled those duties by evaluating the challenged conduct through the lens of the applicable standard of review—business judgment, enhanced scrutiny or entire fairness. *See In re Trados Inc.*, 73 A.3d 17, 42-43 (Del. Ch. 2013).

The business judgment rule is the default standard of review. It presumes that directors operated on an informed basis in honest belief that the action taken was in the best interests of the company. *See Trados*, at 43. Delaware courts review the conduct of a disinterested and independent board for rationality. If the court determines that the action taken lacks any rationality, a court will find liability.

Enhanced scrutiny is the intermediate standard of review. It applies to certain situations where potential conflicts of interest may exist. Under enhanced scrutiny, courts take a closer look at the actions of even independent and disinterested directors. These situations are commonly referred to as *Revlon* and *Unocal* cases, which respectively involved a board resisting a hostile takeover and a company sale. In these circumstances, the court asks whether the action taken was reasonable.

Entire fairness is the highest standard of review and applies where the board is conflicted. Applying this standard, a court asks if the transaction was entirely fair. The court looks to both process and price. Not even an honest belief that the transaction was entirely fair will establish fairness. It is an objective analysis and the board typically holds the burden of proof.

In the Delaware Court of Chancery, a judge makes these determinations either in response to a motion or after trial. This provides more predictability. One chancellor and six vice-chancellors render lengthy, sophisticated opinions.

Delaware corporate law also provides guidance and predictability for boards to consider at the outset of a deal regarding the standard of review or the likelihood that later scrutiny would involve a burden shift. For example, if at the beginning of a deal the board conditions the deal on two procedural devices: a special committee and a majority-of-the-minority vote, those safeguards set

CONTINUED ON PAGE 6

CONTINUED FROM PAGE 5

the standard of review as business judgment. While entire fairness would otherwise apply, Delaware courts acknowledge that the dual protective measures protect minority interests. *See Kahn v. M&F Worldwide Corp.*, 88 A.3d 635, 644-47 (Del. 2014). This structure is significant because it may allow a judge to dismiss a case on a motion, before the cost, stress, and uncertainty of trial.

Outside of Delaware (By Way of Example, New York, Missouri and California)

Outside of Delaware, there tends to be less developed case law. Most states acknowledge the traditional fiduciary duties of care and loyalty. Most states also acknowledge the business judgment rule.

For instance, as the New York Court of Appeals recently observed: "We have long adhered to the business judgment rule, which provides that, where corporate officers or directors exercise unbiased judgment in determining that certain actions will promote the corporation's interests, courts will defer to those determinations if they were made in good faith." *In re Kenneth Cole Prods., Inc.*, 27 N.Y. 3d 268, 274 (2016). So does Missouri. *See Sutherland v. Sutherland*, 348 S.W.3d 84, 90 (Mo. Ct. App. 2011) (under the business judgment rule Missouri will not interfere with "the decisions of corporate officers and directors absent a showing of fraud, illegal conduct, an ultra vires act, or an irrational business judgment").

Outside of Delaware, many states do not recognize an intermediate standard of review. Rather, if the business judgment rule does not apply, many jurisdictions immediately pivot to a fairness analysis. While this fairness analysis varies, fair price and process are typically the focus. For instance, in California, there is "a 'comprehensive rule of 'inherent fairness' which applies alike to officers, directors, and controlling shareholders in the exercise of powers that are theirs by virtue of their position . . ." *Kirschner Bros. Oil, Inc. v. Natomas Co.*, 185 Cal. App. 3d 784, 795 (Cal. Ct. App. 1986). Similarly, Missouri looks to fairness. When evaluating a deal, Missouri considers the manner and timing of the negotiations, the use of an independent appraisal, the use of independent counsel and price. *See Turner v. Ferguson*, 149 F.3d 821, 824-25 (8th Cir. 1998).

But perhaps the biggest differentiating factors between Delaware and non-Delaware actions are (a) the decision-maker (judge or jury) and (b) the timing of a resolution. In many states, a jury would decide these cases and courts are reluctant to dismiss this type of case on a pre-trial motion. For example, in Missouri, although a court has the power to make fairness determinations on a dispositive motion, Missouri courts have observed that "[s]ummary judgment in favor of parties who have the burden of proof are rare, and rightly so." *Turner*, 149 F.3d at 825. This type of question is not normally clear enough to be decided as a matter of law. *See Id*.

By contrast, New York appears to have adopted an intermediate approach. Pre-trial, New York has adopted Delaware's approach in *Kahn v. M&F Worldwide Corp.*, and dismissal is more likely if one knows how to (and wishes to) structure a transaction. *See In re Kenneth Cole Prods., Inc.*, 27 N.Y. 3d at 277-79. If a case survives motion practice in New York, it is important to note that a jury will decide the case.

Finally, demonstrating an interesting approach that appears to slant towards Delaware procedure, recent California case law holds that a breach of fiduciary duty case will be decided by a judge in equity (akin to a Chancery Court proceeding). This is because a breach of fiduciary duty claim in California is deemed to be an equitable claim; therefore, a judge will decide the merits, not a jury. *See Cent. Laborers' Pension Fund v. McAfee, Inc.*, 17 Cal. App. 5th 292, 294-300 (2017). That said, California has yet to acknowledge the Delaware structural approach utilized in cases like *Kahn*.

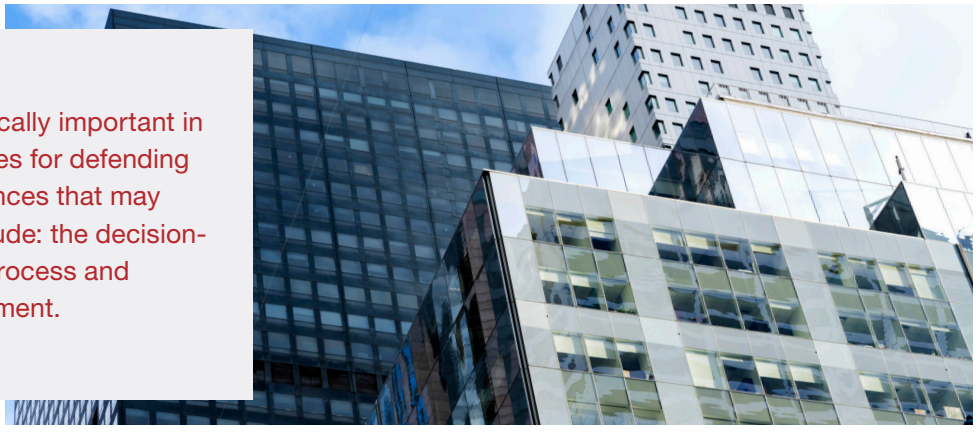
So, what to do?

Jurisdictional differences are critically important in considering the potential outcomes for defending fiduciary duty claims. The differences that may affect the standard of review include: the decision-maker, the length of the judicial process and negotiating leverage in any settlement. To state the obvious, practitioners and clients should consider the impact of different governing laws when incorporating businesses and in structuring M&A transactions.

At the deal table, there are always decisions about structure and process. Creative structuring can ensure that the appropriate and desirable governing law and, as a result, standard of review will apply. Even if a business is already incorporated, actions commonly forming part of an M&A process (such as incorporating an acquisition subsidiary or re-domiciling) present opportunities to modify the otherwise applicable law.

While any expectations should be evaluated with the benefit and context of the applicable deal, a reasonable conclusion is majority stockholders and their controlling director appointees are best served by Delaware courts and governing law. Those courts are more likely to be deferential to the directors' decision-making and protective of the deal. On balance, other state laws may introduce additional uncertainty. This includes the variability of outcomes presented by a jury as the decision maker, which could benefit non-controlling stockholders. Whichever law governs, parties to a deal should be mindful of the impact of that governing law and related court procedures, and should account for the impact when negotiating definitive agreements.

Jurisdictional differences are critically important in considering the potential outcomes for defending fiduciary duty claims. The differences that may affect the standard of review include: the decision-maker, the length of the judicial process and negotiating leverage in any settlement.



CONTINUED FROM PAGE 6

DOL's Narrowing View on ERISA's Fiduciary Indemnification Provisions Raises Risk of Litigation

Few things could more easily bring a cold shiver down the spine of the sponsor of an employee stock ownership plan ("ESOP") than a kindly signed letter from the Department of Labor ("DOL") notifying it that its ESOP is under investigation. After all, it would seem that in this exercise of determining naughty or nice, the DOL more often than not comes bearing a bag of coal. One such common area for DOL criticism is an ESOP's indemnification provisions.

An ESOP is a unique type of qualified retirement plan designed to invest its assets primarily in the stock of the sponsoring employer. Under the Employee Retirement Security Act of 1974, as amended ("ERISA"), the DOL argues that indemnification provisions applicable to ESOP fiduciaries are subject to a stricter standard than that which would apply in the context of other types of qualified retirement plans. ERISA Section 410(a) provides that "any provision in an agreement or instrument which purports to relieve a fiduciary from responsibility or liability for any responsibility, obligation, or duty under this part shall be void against public policy." Notwithstanding this restriction, ERISA 410(b) allows a plan to purchase "insurance for its fiduciaries or for itself . . . if such insurance permits recourse by the insurer against the fiduciary in the case of a breach of a fiduciary obligation." Additionally, a fiduciary may purchase its insurance or an employer may purchase insurance for fiduciaries. *Id.*

Given the special relationship between the employer and the ESOP — i.e., that the ESOP's primary asset is usually stock of the employer — the DOL has been particularly interested in whether an ESOP's fiduciary indemnification provisions allow for an ESOP-owned company to advance a fiduciary's defense costs. If the DOL deems the indemnification provisions to be improper, the DOL takes the position that such indemnification provisions are void. In this eventuality, the fiduciary can end up facing unlimited liability and the need to fund its defense.

Recent Settlements Signal the DOL's Renewed War on the Advancement of Defense Fees

An ESOP must limit the scope of indemnification to preclude indemnification if the fiduciary is ultimately found by a court to have breached its duties under ERISA. The problem with this otherwise clear directive, however, is the winding road to a final court determination that there has been a breach of fiduciary duty. Regarding indemnification, recent DOL enforcement actions have rejected the generally accepted practice of advancing defense costs regardless of whether the arrangement stipulates that the fiduciary must reimburse the fees if the fiduciary is, ultimately found, liable.

The controlling standard, until recently, had been found in *Harris v. GreatBanc Trust Co.*, No. EDCV12-1648-R, 2013 BL 71187 (C.D. Cal. Mar. 15, 2013). There, the court **rejected** the DOL's attempt to void an indemnification provision that allowed the advancement of defense fees by a 100% ESOP-owned company. The DOL argued that enforcement of the indemnification provisions would harm the ESOP because payments of defense costs or indemnification by the plan sponsor would decrease the employer's assets and, therefore, the value of its stock. But, the court disagreed. It held that advancement is permitted if it requires the parties to agree on a reasonably satisfactory repayment mechanism in the event there is a later finding that indemnification is prohibited. Since 2013, the *Harris* approach has become the favored approach and includes the most well-written indemnification provisions to incorporate this language.

Roughly a year ago, however, the DOL signaled its interest in imposing still further restrictions. In a consent order in *Scalia v. Farmers National Bank of Danville*, No. 1:20-cv-674, 2020 BL 87428 (S.D. Ind. Feb. 28, 2020), the DOL took the position that any advancement of fees to an ESOP fiduciary must be preceded by an independent third party's determination that there has been no breach of fiduciary duty — something that will likely be difficult, impractical, expensive and perhaps impossible to obtain. Further, the DOL narrowly construed the repayment mechanism that will be acceptable by suggesting that it will only permit such provisions in which a fiduciary posts collateral or purchases a bond to cover any eventual repayment obligation. Finally, aware that a fiduciary could settle litigation without a finding of liability, the DOL required that the agreement provide that any appreciable settlement amount (i.e., more than a nuisance settlement) result in a full refund of any fees and expenses.

Even more recently, in the matter of *Scalia v. Professional Fiduciary Services, LLC*, No. 7:19-CV-07874-KMK (S.D.N.Y. Jan. 12, 2021), the DOL went a step further in another consent order. There, the DOL blatantly prohibited indemnification agreements that would allow the advancement of fees to fiduciaries in the event a breach of fiduciary claim is asserted. Additionally, the defendants were also prohibited from receiving any indemnification payments or advance payments of legal fees related to a breach of fiduciary claim regardless of any agreements.

While the provisions of the consent orders are only binding on the parties to the agreements themselves, the DOL's approach should serve as notice to all ESOP companies to carefully review their indemnification provisions to maximize the likelihood of enforceability and understand that the restrictions followed by policies focused on the *Harris* standard may no longer be sufficient

CONTINUED ON PAGE 8

CONTINUED FROM PAGE 7

Next Steps

Given the lack of statutory, regulatory, or otherwise published guidance, it is understandable if employers feel unsure as to how to proceed. Nonetheless, the ESOP-owned employer would do well to re-evaluate its indemnification agreements keeping in mind the following:

- **Indemnification by Employer:** If the employer has agreed to indemnify fiduciaries, the employer's focus must be on ensuring that the ESOP's indemnification provisions and any advancement agreements are structured to maximize the likelihood of enforceability in accordance with ERISA. At the very least, advancement agreements must provide for their reimbursement in the event the fiduciary is found to be liable.
- **Indemnification through Insurance:** Alternatively, if the employer is purchasing insurance coverage for the fiduciaries, the first step would be to review the policy and its agreements with the fiduciaries for the following:
  - *Consider the impact of third-party exclusions.* Many policies restrict coverage to fiduciaries that are employees, carving out trustee or financial advisor fiduciaries unless otherwise provided. Therefore, if the fiduciary is a third-party, the employer should modify the policy as soon as possible to provide adequate coverage.
  - *Consider the impact of resignations or removals on indemnification rights.* Given the reach of ERISA fiduciary liability, the employer may want to ensure (or may be required through its fiduciary agreements) to cover a fiduciary even after the fiduciary has been removed or has resigned. The employer should ensure the policy provides tail coverage to cover this situation. Because of the recent DOL proceedings, the cost of fiduciary liability has become more expensive. This could impact an employer's negotiations with a third-party fiduciary who pays for its insurance. Legal help may be needed in the event a fiduciary attempts to negotiate higher administrative fees to cover the costs of purchasing the requisite insurance on its own rather than relying on employer-provided coverage.
  - **Blended Approach:** In the interest of reducing costs, an employer may also consider layering fiduciary coverage. Such an arrangement could entail the employer obtaining primary insurance coverage for the fiduciary with corporate indemnification being secondary. An employer could then reduce its costs further (depending on the employer's facts and circumstances) by only providing indemnification up to a dollar limit and additional insurance for excess amounts.

As a final note, it is important to point out that the above discussion is solely in the context of ERISA indemnification. Because different standards apply, it may be advisable to have separate indemnification arrangements for corporate officers and directors relating to corporate matters. All of these issues involve a high technical application of rules and regulations pertaining to ESOPs and associated fiduciary duties. If you have any questions or concerns, you should strongly consider contacting experienced ESOP counsel.

Mergers and Acquisitions Litigation

Members of Polsinelli's national business litigation practice work in close collaboration with Polsinelli's corporate and transactional attorneys representing buyers, sellers, officers and directors, boards and board committees, founders and other stakeholders in disputes arising from merger and acquisition transactions.

These transactions include a broad cross-section of business organizations, including, among others, Fortune 500 companies, private equity sponsors, venture capital sponsors, nonprofit organizations, manufacturers, foundations, operators and founders.

Contact

Noam B. Fischman
Editor
Chair, M&A Litigation Working Group
nfischman@polsinelli.com
202.626.8360

POLSINELLI