Advocate's EDGE

New litigation frontier

Proving cyber breach damages can be challenging

Why executives pose the greatest occupational fraud risk

Fair value

DCF isn't always appropriate

Making the argument for — or against — alter ego liability

July/August 2015

Arnie & Company

A PROFESSIONAL CORPORATION OF CERTIFIED PUBLIC ACCOUNTANTS

5100 WESTHEIMER, SUITE 490
HOUSTON, TEXAS 77056
(713) 840-1634
FAX (713) 840-1628

New litigation frontier

Proving cyber breach damages can be challenging

Home Depot, Target, TJX and Anthem — all made headlines when their networks were hacked and thieves made off with the personal data of millions of consumers. Not surprisingly, such high-profile cyber breaches usually are followed by lawsuits. Much of the litigation thus far has focused on issues related to damages, particularly actual loss and causation. Here's an overview of how plaintiffs in cyber breach actions have claimed damages and how courts have ruled.

DID THE PLAINTIFF SUFFER?

The most significant problem for many plaintiffs in cyber breach cases is that they haven't yet suffered any losses. For example, thieves may not have had a chance to use the plaintiff's personally identifiable information (PII) to open any fraudulent accounts, withdraw funds or make fraudulent charges. Courts have consistently held that PII itself has no inherent monetary value for which a consumer can be compensated.

To get around this, plaintiffs may seek reimbursements for credit monitoring services or identity theft insurance purchased to combat potential future fraudulent activity using their PII. Numerous courts, however, have denied claims based on the increased risk of future harm — the notion that the breach put consumers at risk of having their PII misused for identity theft, fraud or phishing. And courts have also rejected claims for time and money expended to mitigate the increased risk.

WAS THE DEFENDANT UNJUSTLY ENRICHED?

In March 2014, however, a federal district court approved a $3 million settlement in a data breach case that included plaintiffs who had suffered no financial losses because of identity theft. The district court and the 11th Circuit Court of Appeals found that these plaintiffs had sufficiently pled injury by claiming that the defendant, AvMed, was unjustly enriched because the plaintiffs paid the company more in insurance premiums in exchange for it taking sufficient measures to protect their data.

Similarly, a "benefit of the bargain" approach seems most likely to survive when the defendant has offered assurances that the plaintiff's information would be protected. For example, in 2013, a federal district court allowed a claim against a computer game developer in which the developer had assured customers that it would protect the personal information and private financial information they were required to provide.

Even where plaintiffs can prove misuse of their PII, they can't necessarily recover damages. Damages aren't available for reimbursed monetary losses. For example, if breached credit card information was used to make fraudulent charges, the consumer can't recover damages if the credit card company reimbursed him or her for charges.

DID THE BREACH CAUSE THE LOSS?

Of course, proving sufficient injury isn't enough: A claimant also must establish that his or her injury resulted from the breach. Breaches are common, and consumers share their information constantly online. So making such a connection can be difficult.

A Delaware state court, for example, dismissed negligence claims in a breach case because the plaintiffs had failed to present valid evidence that the breach — and not something else — was the cause of alleged instances of identity theft. But the Ninth Circuit has allowed a claim in which the plaintiff made a detailed showing of factual information supporting temporal and logical relationships between the breach and incidents of identity fraud the plaintiff subsequently suffered.

IS INSURANCE THE SOLUTION?

Data breach insurance — also known as cyber liability or cyber risk insurance — has been around for more than a decade. But interest in these policies has surged in the last couple of years. Not only are companies worried about increasing cyber attack risk, but many insurers are also starting to exclude electronic data losses from traditional corporate policies.

Data breach insurance generally provides three main types of coverage: 1) regulatory fines and penalties, 2) lawsuits and 3) response costs (such as forensic analysis, notification and public relations–related expenses). While the general coverage areas are similar across policies, the devil is in the details.

For example, different policies may have varied approaches to the use of vendors in responding to data breaches. Will the insurer provide the necessary services itself or require the insured to use particular vendors — or can the insured use its own vendors or internal resources?

Premiums and sublimits also warrant close attention. Companies should negotiate sublimits for each coverage area, rather than just an overall limit. Other factors that affect premium rates include an insured's existing security, privacy controls and revenues.

EXPERTS CAN HELP

Both plaintiffs and defendants in cyber breach cases should turn to qualified financial experts for assistance with their damages claims. Damages experts can conduct statistical analyses of fraudulent activities allegedly caused by a breach and examine damages estimates proposed by the opposing party. They also can help determine whether opposing experts used the appropriate time frame when measuring damages and distinguished between the types of fraud that can reasonably be linked to the breach — and those that can't.

Why executives pose the greatest occupational fraud risk

In its 2014 *Report to the Nations on Occupational Fraud and Abuse*, the Association of Certified Fraud Examiners (ACFE) reported that organizations lose an estimated 5% of annual revenues to employee fraud. Although they aren't the most likely people to commit occupational fraud, owners and executives can cause the most damage. So spotting the signs of executive fraud and nabbing these high-placed thieves is critical.

GREATER AUTHORITY EQUALS GREATER DAMAGE

According to the ACFE study, a fraud perpetrator's level of authority generally is proportional to the company's fraud losses. This happens because higher-level employees have greater access to assets and can more easily override internal controls. Owners and executives only accounted for 19% of all cases in the study, but they caused a median loss of $500,000. By contrast, rank-and-file employees committed 42% of fraud schemes but caused a median loss of only $75,000.

> *Financial weakness, credit difficulties and pressure to meet budgets and earnings projections can motivate an executive to do "whatever it takes."*

Executive fraud schemes also tend to continue for longer periods before detection. Where the primary perpetrator was an owner or executive, schemes ran a median duration of two years — twice as long as those involving lower-level employees.

REVEALING SIGNS

So what's a company to do when it suspects executive fraud? Some businesses conduct extensive background checks, but their effectiveness is limited when it comes to occupational theft because most fraudsters are first-time offenders.

Fortunately, executive fraud raises a few red flags. Perpetrators often are reluctant to cooperate with internal investigations and outside auditors and may show disrespect for regulators. They may offer unreasonable responses to reasonable questions or become agitated or annoyed when probed about financial discrepancies.

Their lifestyles also might betray them. A thieving executive may begin spending extravagantly on expensive cars, jewelry or vacations. Or a formerly fiscally healthy individual may appear to be mired in debt and have credit problems. In some cases, the motivation for fraud is a substance abuse or gambling problem, so signs of addiction merit immediate attention.

VULNERABILITIES CREATE OPPORTUNITIES

Certain management and operational factors make executive fraud easier to perpetrate. Primary among them is weak internal controls.

But more specific issues include little or no segregation of duties, little or no external audit oversight, a lax or inexperienced accounting staff, excessive trust in key executives, and an environment where all decisions are made by an individual or small group.

Companies in financial distress, in particular, can provide opportunities for dishonest executives. If the business sells assets for less than their market value, executes an excessive number of year end transactions, routinely rolls over loans or loses important financial documents, it could signal more than inept management. Other warning signs include significant downsizing in a healthy economic environment and a high turnover rate for employees leaving voluntarily.

Some executives commit fraud for what they believe is the benefit of the company. Financial weakness, out-of-control expenses, tax adjustments by the IRS, credit difficulties and pressure to meet budgets and earnings projections can all motivate an executive to do "whatever it takes" to prop the company up. So when bottom-line results seem too good to be true, that just may be the case.

TONE AT THE TOP

Executive fraud can have devastating financial consequences and harm a company's reputation with shareholders and the public. But fraud at the top is dangerous for another reason: It sets the ethical tone for the entire organization. Employees who know or suspect their superiors are dishonest are more likely to cut corners — or commit occupational fraud — themselves. If your clients believe an executive is cheating, don't hesitate to call in a fraud expert to investigate.

Fair value

DCF isn't always appropriate

The Chancery Court of Delaware, the favored state of incorporation for many U.S. companies, regularly uses the discounted cash flow (DCF) method in statutory appraisal cases where the court must determine a corporation's fair value. But as recent case *Laidler v. Hesco Bastion Environmental, Inc.* demonstrates, the court will apply the less common direct capitalization of cash flow (DCCF) method under certain circumstances.

SHAREHOLDER FILES SUIT

The case was brought by a former managing director of one of an affiliated group of companies (operating under common control) involved in the design and manufacture of "Concertainer units." These units are deployable barriers that operate as giant sandbags for military, asset and flood protection.

The former employee held a 10% interest (or 10,000 shares) in another of the affiliated companies known as Hesco. She lost that interest when Hesco merged with another affiliate, Hesco Bastion Environmental. The latter company already owned a 90% interest in Hesco, so no stockholder vote was necessary to consummate the short-form merger.

In January 2012, the former employee was offered $207.50 per share for her interest in Hesco. She declined the offer and filed a petition for a statutory appraisal.

DCCF METHOD CORRECT

The opposing experts both relied primarily on the DCCF method, rather than the DCF method. The latter projects cash flows over a period of time and estimates a terminal value at the end of that time period, assuming that cash flows will continue into perpetuity. Then it discounts the cash flows and terminal value to their net present value. Both experts opined that the DCF method wasn't feasible because Hesco's management never made cash flow projections in the ordinary course of business.

In light of that testimony, the Chancery Court found that the DCCF method was the most reliable indicator of Hesco's fair value due to the lack of management projections upon which to conduct a DCF analysis, as well as the lack of comparable companies or transactions upon which to base an analysis.

Although the experts agreed that the DCCF method was the correct technique, they differed on the appropriate normalized cash flows and capitalization rates to apply.

EXPERTS DISPUTE DCCF INPUTS

The DCCF method involves two steps:

1. Estimating a normalized level of cash flows into perpetuity, and
2. Dividing those cash flows by a capitalization rate to estimate the present value of the business.

Although the experts agreed that the DCCF method was the correct valuation technique, they differed on the appropriate normalized cash flows and capitalization rates to apply.

The court found that the best available estimate of normalized future cash flows was the weighted average actual cash flows from 2009, 2010 and 2011. It declined to reduce its estimate of future cash flows based on Hesco's contention that past revenue was generated by specific events (including the BP oil spill and the so-called "500-year flood") that were unlikely to occur again.

To determine the capitalization rate, both experts multiplied Hesco's weighted average cost of capital (WACC) by its long-term growth rate of 4%. They disputed various inputs in calculating the WACC, however. The court found that the company's WACC was 21.83%. Reducing that figure by the 4% growth rate, the court arrived at a capitalization rate of 17.83%.

The Chancery Court ultimately concluded that the fair value of one share of Hesco was $364.24 — 76% more than the former employee was originally offered. Therefore, she was entitled to more than $3.6 million plus interest at the statutory rate.

CIRCUMSTANCES MATTER

The Hesco case serves as a strong reminder that the particular circumstances of a case play a significant role not only in liability issues but also in the valuation techniques used. Unusual circumstances might require a common valuation approach to be set aside for one that's less common.

Making the argument for — or against — alter ego liability

Sometimes parties with legitimate legal claims realize that their would-be defendants aren't able to pay a damages award. That's when they might attempt to recover from a more solvent party — usually a larger company that's closely associated with the defendant. In such "alter ego" situations, attorneys should hire qualified financial experts to help buttress their arguments.

DETERMINING SEPARATENESS

To establish that one company should be liable for the wrongs of another — for example, that a parent should be liable for a subsidiary — a plaintiff generally must present evidence that the two entities have no separate existence. One of the most significant factors is whether they maintain their own corporate structures with appropriate corporate policies and procedures.

That may not be the case if the entities conduct the same business activity, operate out of the same location or use the same letterhead. Separateness also may be called into question if the entities have officers or directors in common or retain the same attorneys, accountants or other professional advisors.

SIFTING THROUGH EVIDENCE

A financial expert seeking to prove or disprove separateness might scrutinize such evidence as financial statements, accounting records and intercompany transactions. The expert might find that the entities are commingling funds or assets, failing to keep independent accounting records or using the subsidiary entity's funds to pay the debts of the parent's owners, all of which challenge separateness.

The expert also may examine the subsidiary's capital structure and key financial ratios to determine if it's undercapitalized — a sign that the subsidiary is financially dependent on its shareholders or parent company. Among other things, a subsidiary can become undercapitalized as a result of fraudulent intercompany transactions. So it's important to determine whether intercompany transactions are normal, arm's-length business dealings or tools for the parent to divert funds from the subsidiary. Special terms or conditions, for example, may indicate a transaction wasn't conducted at arm's length.

Loan documents and credit ratings can demonstrate financial dependence, too. Is the parent named as the borrower or guarantor on the subsidiary's loan agreements? Does the credit rating used to obtain loans reflect solely the subsidiary's status or also the parent's? If the parent and subsidiary represent themselves as a single entity for credit purposes, alter ego liability might follow.

BUILDING YOUR CASE

Merely being related isn't sufficient for a court to impose alter ego liability. Whether arguing for or against the liability, you'll need a qualified financial expert to study the indicators of separateness and present solid evidence that the house cat is — or isn't — really a lion in disguise.

The experience you need. The service you want.

Whether you are dealing with matters of contract disputes, fraud investigations or other economic damages, you need accountants who have extensive experience in preparing and presenting complex commercial cases. In other words, you need Arnie & Company.

For more than a decade, our firm has provided the legal community, business owners and other individuals throughout Texas with prompt, accurate and effective accounting, consulting and litigation support services that include:

- Contract dispute and analysis
- Fraud investigations
- Lost profit analysis
- Securities claims
- Shareholder derivative actions
- Purchase/Sales agreement warranty claims
- Legal and accounting malpractice claims
- Intellectual property analysis
- Other economic damage claims

Arnie & Company has an especially strong depth of experience in the analysis of commercial damages and in conducting forensic investigations. Dennis Arnie is both a Certified Public Accountant and a Certified Fraud Examiner. He has frequently testified as an expert witness in a variety of state and federal courts and various arbitration hearings.

Thanks to the firm's commitment to delivering outstanding service, Arnie & Company has become a trusted advisor to many leading law firms and businesses in the Houston, Dallas, and Austin areas. Our clients include numerous Fortune 500 companies in various industries, as well as significant privately held companies and individuals.

We welcome the opportunity to put our experience and advanced knowledge of commercial damage analysis and forensic accounting to work for you and your clients. Please call us at 713-840-1634 and let us know how we can be of assistance.

Arnie & Company

A PROFESSIONAL CORPORATION OF CERTIFIED PUBLIC ACCOUNTANTS

5100 WESTHEIMER, SUITE 490
HOUSTON, TEXAS 77056