On Damages…

Risk Exposure as an Element of Damages in Financial and Privacy Litigation

January 2020

Introduction

When weighing the viability of a legal claim, and in particular the recoverability of compensatory damages, we make a habit of concentrating on the *tangible consequences* of the alleged misconduct.

This is a natural tendency, as the consequences of the alleged misconduct are typically known: a car was stolen or a victim was wounded. But we have come to apply this shortcut as if it were a rule, despite the fact that the shortcut fails in certain areas. In fact, several courts have defaulted to assuming that a cognizable showing of economic harm is required, rather than investigating whether it is required.

As discussed herein, in data breach cases some courts have devoted themselves, early in the proceedings, to the tangible consequences of the alleged misconduct – *Were the plaintiffs victims of identity theft?* – as opposed to the immediate byproduct of the misconduct.

Specifically, when misconduct exposes plaintiffs to undue risk, the undue risk exposure is the immediate ramification. Tangible consequences, like identity theft, may or may not come to pass, and may take years to play themselves out. The right question is not whether the plaintiffs were all victims of identity theft, but whether they were all similarly exposed, by the alleged misconduct, to identity theft (or any of the various other known and unknown negative consequences of a data breach).

In this article, I will endeavor to explain two broad points:

1. When a defendant's misconduct leads to his enrichment, a plaintiff may be entitled to compensation even if the plaintiff has not suffered, or has not *yet* suffered, traditional monetary losses.
2. The suffering of immediate, tangible losses is not the only appropriate component of damages worth considering: being denied an opportunity to profit (reduced upside) or being exposed to an undue risk (increased downside) may give rise to liability, regardless of whether the profit opportunity materializes (on the upside) or the risk event transpires (on the downside).

AUTHOR

Gene Phillips
Director
gene.phillips@pf2se.com

Direct v. Indirect Damages

Damages can take various forms. I will generally refer to *direct damages* as those that relate directly, or specifically to the misconduct at issue. *Indirect damages* will encompass all other damages, such as incidental or consequential damages.

If a person is physically injured by a neighbor's misdirected fireworks display, I will call the physical harm suffered the direct damages. There may also be indirect damages of a pecuniary rather than a physical nature, including hospital costs, wages foregone during any hospital stay, or any temporary or permanent reduction in salary owing to the injury.

Importantly, any victim's decision-making and performance after the fight (for example his choosing whether or not to go to the hospital or address any wounds) can have an impact on the overall damages, particularly the indirect damages.

Damages in the Absence of Traditional Monetary Losses

Damages are often the central focus of financial and privacy litigation. But what is the *damage* if the plaintiff did not necessarily suffer tangible losses? The alleged misconduct may only rob a plaintiff of an opportunity, or expose her to an undisclosed risk that does not manifest in losses being realized. Nevertheless, the plaintiff may be entitled to compensation.

Suppose a defendant's misconduct denies a plaintiff an opportunity to participate in a bet or a trade (e.g., buying an allotment of a private company's shares at a discounted price per share). Even if the bet or trade, had it been placed, would not ultimately have resulted in a successful outcome, the plaintiff might nevertheless have a claim for a "lost opportunity." Such a claim might look to value of the forgone opportunity at the time of the misconduct, rather than whether the lost opportunity actually proved successful in reality.[1]

The concept of an *increased exposure to risk*, central to this article, is simply the mirror image of a *lost opportunity to profit* – and it should be similarly availing without requiring a deep analysis of the subsequent outcome of the risks taken.[2]

I next explore the economics of lost profit opportunities and heightened risk exposures by way of three thematic examples.

---

[1] Analysis real-world outcomes may not be necessary for tortious claims of lost opportunities, which rest rather on the point-in-time analysis, of value lost, at the moment the opportunity was denied. In Australia, for example, a claim for the loss of a valuable commercial opportunity does not require a plaintiff to show (1) actual pecuniary loss; (2) that she would indeed have participated in the forgone opportunity; or (3) that the opportunity would have resulted in a definite profit, had she participated in it. The lost opportunity is recognized as compensable damage *in and of itself*. See *Sellars v Adelaide Petroleum NL*. (1994) 179 CLR 332, 355. ("… [d]amages for deprivation of a commercial opportunity, whether the deprivation occurred by reason of breach of contract, tort or contravention of s. 52(1), should be ascertained by reference to the court's assessment of the prospects of success of that opportunity had it been pursued.")

[2] At least they are the same in an economic sense. A robbed chance to make a dollar's profit is no different from an unconsented-to exposure to a dollar's loss. Note that both look to chance-based possibilities, rather than the tangible outcomes of events. It may be argued that *tangible harm* occurs at the moment monies are placed at risk or at heightened risk. The focal lens of this section, however, is backward looking, considering traditional monetary losses to be absent when risks do not occur and losses are not *realized*. Thus, I am not suggesting that no tangible injury has occurred when undue risks are taken; rather, I am suggesting that misconduct can sometimes give rise to liability even in the absence of traditional monetary losses ultimately being realized.

Theme 1: The Gambling of Escrowed Accounts

Suppose a trustee or other intermediary to a transaction were to gamble with amounts held for others in trust, or in an escrow account. The gamble might pay off. The gambler might double her money and refill the trust account; or not, if the gamble fails.

We should not limit our concern here to the scenario in which the gamble fails: the real problem is that a gamble took place.

As a financial and legal system we cannot have intermediaries gambling with funds that are supposed to be safeguarded. Regardless of whether the gamble succeed, the moment that trust funds are gambled, the *true owners* are being placed at risk without their permission.

In lodging the bet with someone else's money, the intermediary-gambler takes a risk that was not hers to take, positioning herself to make a profit for her benefit while exposing others to potential losses emanating from the gamble.[3]

As to damages, even if the gambler-intermediary were to succeed and refill the coffers, the exposed parties might nevertheless lodge a claim to claw back some or all of the gambler's ill-gotten profits made by placing their money at risk.[4] Misconduct occurred: an unauthorized risk has been taken.

Related Example: Litigation Concerning Abacus 2006-10

UK-based asset management firm, Astra Asset Management, invested in a structured finance investment (a so-called CDO entitled Abacus 2006-10) which was sponsored by Goldman Sachs. In the litigation that ensued, Astra asserted that Goldman had directed the purchase of collateral for the deal in a manner that violated the deal's applicable eligibility criteria. (*In the Matter of: The trusteeship created by Abacus 2006-10 Ltd. and Abacus 2006-10, Inc., relating to the issuance of Notes pursuant to an Indenture dated as of March 21, 2006*. Court File No. 62-TR-CV-18-39.)

The collateral nonetheless appreciated in value by over $55 million, which Goldman sought to keep for itself.

Astra argued that the investment bank benefited financially from the allegedly undue risks taken, while Astra and other investors in the Abacus CDO bore the risks associated with the investment decisions. As a result, Astra sought to terminate the CDO, require the redemption of all investors at par, and distribute the $55 million to the deal's investors.

The matter was resolved on the eve of trial, for an undisclosed settlement amount.

---

[3] Brokers would typically ask for consent before using idle cash to make investments for the broker's gain. An excerpt from Schwab's agreement reads: "**Float Disclosure**. You agree that Schwab may retain as compensation for services your Account's proportionate share of any interest earned on aggregate cash balances held in Schwab's bank account with respect to (1) assets awaiting investment or (2) assets pending distribution from your Account. Such interest retained by Schwab shall generally be at money market rates." (emphasis in the original) Fidelity's agreement includes the language: "Subject to applicable law, Fidelity may use this free credit balance in connection with its business. Fidelity may, but is not required to, pay you interest on this free credit balance …"

[4] Suppose the parties whose money was held in trust wanted to gamble their monies. Had their bets paid off, they would have been the beneficiaries – not the gambler-intermediary.

Theme 2: Financial Markets and Insurance/Credit Products

Suppose a person were to lie to an insurer about her health so as to procure a cheaper health or life insurance policy, or lie to a credit provider about her financial position to secure a more affordable home loan. The insurance company or credit provider may be able to nullify (or rescind) the contract immediately upon discovering the lie: the insurer need not wait for her to fall ill before taking action, and similarly the credit provider need not wait for a missed loan payment.

Why? What is it that enables the insurer or credit provider to adjust or rescind a contract before it has suffered tangible losses – and what enables us to ascertain whether the lie was material? The answer lies in the concept of *risk*.

In the financial markets, the *reward* sought is often tied to the level of *risk* taken.

To make this concrete in financial terms, suppose a company raises funds at a yield of 5% based on artificially inflated financials, where 7% should have been the proper compensation (reward) based on the company's true financials. Any investors earning *only* 5%, despite taking a "true" risk consistent with a 7% return, would have suffered damages even if all promised 5% payments were made. No default or payment failure is required: the economic damage has already come to pass in that there was a failure to properly compensate investors for the true risk taken (i.e., they should have received a 7% return).

Example: Citigroup Bond Litigation

Towards the end of 2008, in the near aftermath of Lehman Brothers' collapse, investors in roughly 50 of Citigroup's bond and preferred stock offerings combined to sue the firm and certain individuals. (*In re Citigroup, Inc. Bond Action Litigation*; 08-cv-9522)

At the time the class action was initiated, Citigroup had not defaulted on its bonds, but the market values associated with the bonds had declined substantially since issuance.[5]

Plaintiffs' amended complaint included 7 causes of action. The claims lodged were not fraud-based allegations, but rather constructed along the following lines:

- Plaintiffs had purchased the bonds based on information in the offering documents, which contained untruths, omissions, or misleading statements;
- Plaintiffs "did not know, or in the exercise of reasonable diligence could not have known..." of the untruths, omissions, or misleading statements;
- The "value of the Bond Offering Securities has declined substantially subsequent to the consummation of the Offerings"; and
- The plaintiffs had suffered damages.

Count 5, for example, includes the following language:

> "This claim does not sound in fraud. For purposes of asserting this claim under the 1933 Act, Plaintiffs do not allege that Defendants acted with scienter or fraudulent intent, which are not elements of a Section 12(a)(2) claim.

[5] A substantial decline in market value is often consistent with the marketplace's realization that the bonds are relatively riskier.

[…]

By virtue of the conduct alleged herein, the Underwriter Defendants violated Section 12(a)(2) of the Securities Act. Accordingly, Plaintiffs and other members of the Class who purchased in Offerings pursuant to the Shelf Registration Statements and incorporated Public Offering Materials have the right to rescind and recover the consideration paid for their securities, and hereby elect to rescind and tender their securities to the Underwriter Defendants and the Underwriter Defendants. In addition, Plaintiffs and the members of the Class who have sold their securities that they originally purchased through the Offerings are entitled to rescissory damages."

The parties would agree to a $730 million settlement, which the court subsequently approved.[6]

Theme 3: Data Breaches

The concept of risk-based exposure applies equally in data breach cases, where a company's misuse of, or failure to protect, customers' (or employees') data results in their data being compromised.

Suppose a company fails to adequately protect its customers' personal data. A hacker breaches the company's inadequate security and steals this data. Here, the indirect damages might include identity theft and other types of fraud suffered by each individual customer, which stem from misconduct *after* the data breach, rather than damages incurred *directly* from the breach (increased risk exposure). Indirect damages, from post-breach misconduct, may be different for different customers, and each customer may take different precautions. Ultimately, for example, the hacker might empty some customers' bank accounts, but leave other smaller accounts untouched.

Courts have sometimes considered complex damages issues such as these early in data breach case proceedings – before discovery has even begun – focusing curiously on the different ways in which customers have responded to their data being compromised. Courts have used the differences in responses to deny standing in class action lawsuits, owing to a lack of commonality in damages.

- ***Dolmage v. Combined Ins. Co. of Am.***[7] In this case, the defendant (Combined Ins.) offered a variety of insurance products to customers, including the plaintiff (Dolmage). One of the defendant's vendors (Enrolltek) posted online social security numbers and other personal information pertaining to the defendant's customers. The plaintiff filed this action alleging breach of contract against Combined Ins. for failing to protect her personally identifiable information. The court denied class certification because the court determined it was necessary to individualize damages, which defeated the commonality required among class members to litigate as a class: "[O]f the 4,000 plus proposed class members, some (like Plaintiff) may have become the victim of an actual theft of funds. A subset of these individuals may have been able to resolve the problems quickly or obtain reimbursement from banks and other third parties. […] Another subset […] suffered emotional distress worrying that they could become a victim of identity theft. Still others may have suffered no distress or inconvenience whatsoever."

- ***In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.***[8] Here, Hannaford grocery store customers' debit and credit card data were stolen in a cybersecurity breach. Plaintiffs (the

[6] Case No. 1:08-cv-09522-SHS, Document 180

[7] *Dolmage v. Combined Ins. Co. of Am*. No. 14 C 3809, 2017 WL 1754772 (N.D. Ill. 2017)

[8] *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig*. 293 F.R.D. 21, 33 (D. Me. 2013)

customers) moved for class certification to pursue claims for various expenses, including to pay for identity theft insurance and credit monitoring. The court's language differed markedly from *Dolmage*, but its ruling similarly considered damages stemming from post-breach misconduct (i.e., indirect damages). In *Hannaford*, to their detriment, plaintiffs provided no expert opinion as to their total damages, which the court found to be fatal. The court's reasoning is noteworthy: "Without an expert, [plaintiffs] cannot prove total damages, and the alternative (which even [plaintiffs] do not advocate) is a trial involving individual issues for each class member as to what happened to his/her data and account, what he/she did about it, and why."

- ***Lloyd v. Google LLC***.[9] Google was accused of tracking the behavior of iPhone users, without their knowledge or consent. The iPhone users brought a collective action lawsuit against Google. The UK High Court concluded that a collective action was inappropriate because of differences among the quality of each class member's data and differences among class members' attitudes towards their data (some valued their personal data more than others).[10]

The *Dolmage, Hannaford* and *Google* courts likely erred in focusing too heavily on (1) the attitudes of the plaintiffs towards their data[11] and (2) any post-breach conduct or post-breach responses to the data breach.[12]

Specifically, these courts examine events *after* the misconduct took place, ruling that differences in indirect damages suffered by individual class members preclude the class from litigating as a group, because these differences frustrate the requirement of commonality among class members.

The real concern should instead be that the data breaches caused direct damages: increased risk exposure. Looking at these rulings through the lens of *increased risk exposure*, the shortcomings may be easier to understand.

The plaintiffs, through the defendants' failure to protect their personal data, have been exposed to risks. Of course, risks linger, meaning that certain indirect damages can materialize well into the future.[13] But that should not affect the ability of a class to seek redress for misconduct that has already occurred.

---

[9] *Lloyd v. Google LLC* [2018] EWHC 2599 (QB)

[10] The UK High Court denied relief on the basis that the damages sought were improper under the particular statutory claims asserted. This ruling was subsequently reversed by the Court of Appeal, as discussed within.

[11] My belief is that class members' attitudes towards data are entirely irrelevant in this context. Data is a commodity, like gold or art; it is regularly traded, and there is a private market for it. Data has a market value regardless of the value that individual class members may ascribe to their data.

[12] Plaintiffs' various post-breach mitigating actions are immaterial to the issue of *commonality*. The commonality criterion seeks to ensure that putative plaintiffs, can adequately be represented by a lead plaintiff: they must share a common injury or common interest in the outcome of the litigation. Here, variations in post-conduct responses are unrelated to the nature of their injuries or their relative interests in the outcome of any subsequent litigation. Suppose several people are struck by someone who wildly swings a baseball bat. Some may incur an injury, while others may not, and the seriousness of their injuries will differ: some may even go hospital. These are real differences, but they are differences that impact the *extent* of damages (in dollar terms) — not the commonality of their injuries. See also footnote 14.

[13] In the event of a data breach we may not know whether someone has suffered indirect damages from the breach (yet) or whether they might still suffer over the coming years.

My contention is that *direct damages* are the most appropriate and effective measure of damages for the purposes of ascertaining commonality for class certification, and that these courts have erred in investigating *indirect damages* while ignoring *direct damages*.[14]

The defendants are being sued for their specific misconduct, which itself is well-defined and consistent (the *direct damages* component); meanwhile the lingering risks, and plaintiffs' responses and mitigating conduct (the *indirect damages* component) are and almost always will be different when you consider any sizeable class of individuals or entities.[15]

Moreover, by neglecting direct damages, these courts have seemed to require a showing of indirect damages (e.g., whether a data breach resulted in people suffering from identity theft) often before those indirect damages can be identified.

The UK High Court's ruling in *Google* would be reversed by the Court of Appeal in October 2019. The Court of Appeal's judgment included strong language that sought to rectify the lower court's focus on the attitudes of the putative class members and their indirect damages:

- Concerning commonality: "[on] the case pleaded, every member of the represented class has had their data deliberately and unlawfully misused, for Google's commercial purposes, without their consent and in violation of their established right to privacy."
- Concerning the lower court's examination as to the different circumstances and attitudes of class members and the impact (if any) from the alleged misuse of their data: "In my judgment, this approach misunderstands the nature of the damage alleged. [The representative plaintiff] alleges that each member of the class has sustained a loss of control as a result of the breach alleged. Each claimant has lost something valuable, namely the right to control their private [browser-generated information]."

[14] This is not to suggest that indirect damages should not be among the distinguishing factors in awarding overall damages. In resolving the *Equifax* data breach litigation, for example, a settlement fund was set up to compensate class members based upon, to a degree, their indirect damages. "Equifax will pay $380,500,000 into a fund for class benefits, attorneys' fees, expenses, service awards, and notice and administration costs; up to an additional $125,000,000 if needed to satisfy claims for certain out-of-pocket losses; and potentially $2 billion more if all 147 million class members sign up for credit monitoring." Specific benefits available to the class members include: "Reimbursement of up to $20,000 for documented, out-of-pocket losses fairly traceable to the breach, such as the cost of freezing or unfreezing a credit file" and "Compensation of up to 20 hours at $25 per hour (subject to a $38 million cap) for time spent taking preventative measures or dealing with identity theft." (*In re: Equifax Inc. Customer Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT, MDL Docket No. 2800)

[15] By way of comparison, consider the court's language at motion to dismiss in the *Facebook* litigation concerning the Cambridge Analytica scandal, which narrows in on the alleged misconduct specific to Facebook: "… contrary to Facebook's argument, the plaintiffs do not seek to hold Facebook liable for the conduct of the app developers and business partners; they seek to hold the company liable for its own misconduct with respect to their information. Specifically, the plaintiffs allege that they entrusted Facebook with their sensitive information, and that Facebook failed to use reasonable care to safeguard that information, giving third parties access to it without taking any precautions to constrain that access to protect the plaintiffs' privacy, despite assurances it would do so. This lawsuit is first and foremost about how Facebook handled its users' information, not about what third parties did once they got hold of it." (*In Re: Facebook, Inc., Consumer Privacy User Profile Litigation,* Case No. 18-md-02843-VC, Doc. 298, p. 36)

Closing Remarks

The showing of damages (for example for the purposes of standing under *Spokeo* in the United States[16]) can be satisfied in a number of ways. Exposing a plaintiff to increased risk may be one way to demonstrate damages.

Whether we are considering financial-market or data-related litigation, it is worth appreciating that damages are not always financial in nature;[17] and that even when they are, they need not rely on a showing of financial losses being *realized*.

Investors purchasing securities based on artificially inflated financials – for example, when material risks go undisclosed or "under-disclosed"[18] – have long been able to bring disclosure-related claims. The risk element, itself, is enough. In data breach cases too, increased exposures to economic risk should similarly give rise to a viable claim, regardless of whether indirect damages have crystallized. Risk-based direct damages can be tangible or intangible; they are often complex in nature; and they can be difficult to value in cases like data breach cases. But they are central to the issues and should not be ignored.

One caveat, of course, is that courts will likely shun claims for risk-based compensation when the risks are seen as too speculative or indefinite.[19] The risks need to be relatively specific, i.e., measurable or economic.

So how do we know when a risk is measurable or economic?

To fully answer this question likely requires an article of its own; one basic mechanism, albeit imperfect, is to consider that a risk may be measurable or economic if one would need to pay to protect against its occurrence.

---

[16] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016)

[17] Consider, *Thole v. U.S. Bank, N.A*. No. 17-1712, which was recently argued before the U.S. Supreme Court (Jan. 2020). At issue, to a degree, is whether petitioner-plaintiffs have standing if their rights are "adversely affected" *absent* individual financial harm being suffered. This litigation pits various circuit court rulings against one another, in determining whether individual monetary loss (or risk thereof) is necessary to sue for a specific fiduciary breach. Respondents argue that "Because Plaintiffs' benefits are fixed […] purported Plan losses have had (and will have) no effect on Plaintiffs themselves" and that petitioner-plaintiffs have suffered no concrete injury from respondents' misconduct. Petitioner-plaintiffs argue *inter alia* that for an injury to be "concrete" it need not be a financial injury. (Brief of respondents U.S. Bank, N.A., et al. in opposition, filed Aug. 22, 2018; and Reply of petitioners James J. Thole, et al., filed Sept. 5, 2018)

[18] The nature of the risk may be disclosed, but the extent of the risk may, misleadingly, be diminished. For example, the SEC recently charged Facebook (July 2019) with stating a certain challenge as a business risk, when Facebook allegedly already knew that the risk had already materialized. "For more than two years, Facebook's public disclosures presented the risk of misuse of user data as merely hypothetical when Facebook knew that a third-party developer had actually misused Facebook user data. Public companies must identify and consider the material risks to their business and have procedures designed to make disclosures that are accurate in all material respects, including not continuing to describe a risk as hypothetical when it has in fact happened." https://www.sec.gov/news/press-release/2019-140

[19] A drunk driver might expose a random pedestrian to increased risk of injury, but unless that pedestrian is actually struck by the driver's car, she likely would not have a claim. The risk is too hypothetical in nature, and she could simply limit the risk by crossing the road or moving elsewhere so as to avoid injury. The act of crossing the road (risk reduction) would not have come at any considerable cost.

In the aftermath of a data breach, for example, a concerned individual might hire a credit monitoring agency to alert her to any unusual account activity, or she might purchase identity theft insurance – which would leave me to think that these risks would be considered to be real, measurable, economic. There is a marketplace for the hedging of these risks.

Oddly, the fact that some class members had already suffered knock-on consequences of the breach, while others had not, encouraged some courts to deny class certification. But from a different perspective, the same facts also show that the risks they were all exposed to by the same misconduct are actually real and finite, in support of an argument for standing. That some parties exposed to a data breach actually suffered from identity theft in fact particularizes the risk: it is less hypothetical in that it has already transpired for some people in the population exposed.

The task for litigators and judges in cases like data breach cases is to understand whether the alleged misconduct directly introduced new or heightened economic risks – rather than looking only to indirect damages, which may only occur in the future (or not). A distinction has to be made.

* * *

PF2 Securities' research team focuses on the dynamics of financial markets and complex products. We are typically engaged in the context of dispute resolution or litigation to explain market norms from a practitioner's perspective; build or apply mathematical models and statistical techniques to analyze (potentially anomalous) market movements and patterns; and to quantify potential damages from any alleged or agreed-upon wrongdoing. PF2 Securities has offices in New York, Los Angeles, and Sydney.

For North American or European matters, email us at info@pf2se.com, or for Australian matters at info@pf2se.com.au.

You can join our distribution list by signing up on the News & Research page of our website. Or follow us on LinkedIn: https://www.linkedin.com/company/pf2-securities-evaluations/