THOMSON REUTERS
Westlaw®

Damages: risk exposure as an element of damages in financial and privacy litigation

By Gene Phillips, *PF2 Securities**

JULY 16, 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.

Some courts overseeing data breach cases 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.

In this article, I will endeavor to explain why the right question is not whether the data breach plaintiffs were ultimately victims of identity theft. Rather, when misconduct exposes plaintiffs to undue risk, it is the undue risk exposure that is the immediate consequence.

DIRECT V. INDIRECT DAMAGES

Damages can take various forms.

I refer to *direct damages* as those that relate specifically to the misconduct at issue. If a person is physically injured by a neighbor's misdirected fireworks display, the physical harm suffered would be the direct damages.

Indirect damages encompasses all other damages, such as incidental or consequential damages. Indirect damages are of a pecuniary rather than a physical nature, including hospital costs, wages foregone during any hospital stay, or any reduction in salary owing to the injury.

Importantly, a victim's decision-making and performance after the event (e.g., his choosing whether or not to go to hospital) 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 are the *damages* 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 realized losses.

Suppose a defendant's misconduct denies a plaintiff an opportunity to participate in a venture or trade. Even if the venture 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 to profit*.

> The moment that trust funds are gambled, misconduct has occurred: the *true owners* are being placed at risk without their permission.

The concept of an *increased exposure to risk*, central to this article, mirrors the argument of a *lost opportunity to profit* — a robbed chance to make a dollar's profit is economically no different from an unconsented-to exposure to a dollar's loss.

Importantly, both approaches concern themselves with alleged misconduct that gives rise to liability, not the outcome of the alleged misconduct.

THEME 1: FINANCIAL AND INSURANCE PRODUCTS AND CONTRACTS

Suppose a person were to lie to an insurance company about her health so as to procure a cheaper policy, or lie to a credit provider about her financial position to secure a more affordable home loan.

The insurer 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 the credit provider need not await a missed loan payment.

What is it that enables the insurer or credit provider to adjust or rescind a contract before it has suffered tangible losses? 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 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.

> Data has a market value regardless of the value that individual class members may ascribe to their data.

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. (See *In re Citigroup, Inc. Bond Action Litigation*, 08-cv-9522, which resulted in a court-approved settlement of $730 million.)

THEME 2: 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. But we should not limit our concern here to the scenario in which the gamble fails: the real problem is that a gamble took place.

The moment that trust funds are gambled, misconduct has occurred: the *true owners* are being placed at risk without their permission. Even if the accounts are refilled, 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. (See *In the Matter of: The trusteeship created by Abacus 2006-10 Ltd. and Abacus 2006-10, Inc.,* Court File No. 62-TR-CV-18-39.)

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 hacker breaches a company's inadequate security and steals its customers' data.

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 alleged misconduct by the company, which may have been negligent in exposing its customers to the hack event.

Indirect damages, from post-breach misconduct, may certainly differ from one customer to the next, and each customer may take different precautions. Ultimately, for example, the hacker might empty some customers' bank accounts, but leave other accounts untouched.

Courts have sometimes examined 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.* No. 14 C 3809, 2017 WL 1754772 (N.D. Ill. 2017).** Defendant Combined Ins. offered a variety of insurance products to customers, including plaintiff Dolmage. One of the defendant's vendors (Enrolltek) posted online defendant's customers' social security numbers and other personal information. 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, deciding that it was necessary to individualize damages: "[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.* 293 F.R.D. 21, 33 (D. Me. 2013).** Hannaford's customers' debit and credit card data were stolen in a cybersecurity breach. The customer-plaintiffs 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). 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* [2018] EWHC 2599 (QB).** 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).

First, the *DoImage, Hannaford* and *Google* courts likely erred in concerning themselves with events that took place *after* the alleged misconduct. The putative plaintiffs' various post-breach mitigating actions are immaterial to the issue of commonality.

Rather, the spirit of the commonality criterion is to ensure that plaintiffs can be adequately represented by a lead plaintiff: they must share a common injury or common interest in the outcome of the litigation.

> Exposing a plaintiff to increased risk may be one way to demonstrate damages.

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.

Second, differences among the putative 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.

The courts should instead have been by focused on the direct damages which are in fact common among the plaintiffs. 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 the same risks in the same way.

Risks linger, meaning that certain indirect damages can materialize well into the future; but that should not jeopardize the ability to seek redress for misconduct that has already occurred.

Fortunately, not all courts have allowed the *indirect* damages to detract from the critical *direct* damages.

In the *Facebook* litigation concerning the Cambridge Analytica scandal, the court homed in on the allegations 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)

The above mentioned UK High Court's ruling in *Google* would later 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 misplaced attention:

- 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 of different circumstances and attitudes among the class members: "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]."

CLOSING REMARKS

The showing of damages (for example for the purposes of standing under *Spokeo* in the United States) 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; 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" — 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. 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.

In the aftermath of a data breach, for example, a concerned individual might hire a credit monitoring agency or she might purchase identity theft insurance — each of which would leave me to think that these risks would be considered to be measurable and 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.

This article appeared on the Westlaw Practitioner Insights Commentaries webpage on July 16, 2020.

ABOUT THE AUTHOR

Gene Phillips is a director at **PF2 Securities**. He and his colleagues consult on complex litigation matters, particularly when financial firms, markets or products are involved, and advise on financial concepts like valuations and damages calculations. Phillips heads PF2's litigation consulting business and is based in Los Angeles. PF2 has offices in New York, Los Angeles and Sydney. He can be reached at gene.phillips@pf2se.com. A version of this article was originally published on PF2's website, www.pf2se.com. Republished with permission.