INFORMATION LAW JOURNAL

A Publication of the Information Security and EDDE Committees
ABA Section of Science & Technology Law

WINTER 2016 VOLUME 7 ISSUE 1 EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.

Economic Analysis of Financial Institution Claims in Data Breach Class Actions

By Michael Kheyfets, Matthew Milner, and Andrew Sand

Data breaches—that is, the unauthorized access to, or disclosure of, personal data—are quickly becoming a reality of doing business for many companies. Many corporate data breaches are now also closely followed by class action lawsuits against the breached company. While much of the analysis in this area of litigation has focused on consumer cases—brought by the customers of the breached businesses—courts in those cases typically grapple with the issue of legal standing for plaintiffs. Less analysis has been done of institutional cases, for example involving banks filing a suit after *Read more*

Active Response Continuum

By Wesley Paisley

Companies have always needed a defense against cyber thieves, cyber terrorists, and other miscreants to protect their intellectual property. With the recent attacks on Ashley Madison and a Vermont aero dynamics firm, companies need to take offensive measures to protect their stolen property. Governments and non-governmental organizations are not the only targets for cyber espionage. Companies generally have a duty to make sure their physical/cyber space is secure, therefore they should be able to use offensive measures to uphold that duty. *Read more*

Privacy in the Cloud - Are the unique privacy obligations of Federal agencies raising the bar for cloud provider security practices across the commercial marketplace?

By Michael A. Aisenberg

Trust on the Internet may seem to have been in short supply for quite a while. Data breaches abound; governments and others we rely on to safeguard our personal data from the web are losing control over it or subjecting it to extreme and unauthorized analytics and exchanges. A “lot’ of individual data certainly must now exist in the storage of entirely unexpected systems, controlled by entirely unauthorized parties. Facebook’s present storage array is reputedly growing from 10^{15} to some multiple. Exabytes (10^{18}) is likely way too small a measure of cumulative storage implicated *Read more*

The City of Big Shoulders Looks to be the City of Big Data

By Nicholas P. Brankle

Big Data is all around lately. As more of our lives go online, information about how we live and interact with one another and with our environments continues to proliferate. Businesses and academics comb through big data to find previously unseen patterns and to seek out clues to previously unanswerable questions. It was only a matter of time before cities sought to harness the power of big data to see what they might be able to do with it. That time is now. Chicago will soon launch the Array of Things, a big data project that is meant to measure and take the pulse of the city and its residents and *Read more*

2015 (2H) Information Law Updates: Cases, Statutes, and Standards

By Thomas J. Shaw

In the second half of 2015 and the end of the first half, there have been many developments in U.S. and international information law cases, statutes, and standards. These development include international and U.S. state and federal statutes and regulations passed or coming into force, civil and criminal cases and enforcement actions brought by regulators, and new standards, guidelines, and legal ethics opinions in this area. To briefly summarize the major developments in this area of law and practice, each significant development is presented with a brief analysis describing it. *Read more*

Economic Analysis of Financial Institution Claims in Data Breach Class Actions

By Michael Kheyfets, Matthew Milner, and Andrew Sand

Data breaches—that is, the unauthorized access to, or disclosure of, personal data—are quickly becoming a reality of doing business for many companies. Many corporate data breaches are now also closely followed by class action lawsuits against the breached company. While much of the analysis in this area of litigation has focused on consumer cases—brought by the customers of the breached businesses—courts in those cases typically grapple with the issue of legal standing for plaintiffs.

Less analysis has been done of institutional cases, for example involving banks filing a suit after information on payment cards they issued is disclosed in a breach. Claims brought by financial institution plaintiffs, however, have thus far been less susceptible to the jurisdictional hurdle of legal standing and several have proceeded to the class certification phase.

In this article, we specifically focus our analysis on litigation matters filed by financial institution classes. We first summarize the types of harms plaintiffs typically claim in these matters and focus on how the characteristics of these cases might differ from their consumer counterparts. We also discuss an economic framework relevant to the evaluation of damages claims in financial institution cases and highlight important considerations relating to economic analysis of these cases in the class action context.

I. INTRODUCTION

In July 2015, Home Depot filed a motion to dismiss a consolidated class action complaint brought against it by a group of financial institutions ("FIs") relating to one of the largest retailer data breaches in history.[1] It is believed that between April and September 2014, hackers compromised approximately 56 million unique payment cards[2] as well as approximately 53 million email addresses[3] in Home Depot's information systems. The breach was first publicized in September 2014,[4] and at least

[1] Memorandum of Law in Support of Home Depot U.S.A., Inc. and the Home Depot, Inc.'s Motion to Dismiss the Financial Institution Plaintiffs' Consolidated Class Action Complaint, In re: The Home Depot, Inc., Customer Data Security Breach Litigation (No. 1:14-02583-TWT) (N.D. Ga. filed July 1, 2015).

[2] *The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores*, September 18, 2014. Available at http://media.corporate-ir.net/media_files/IROL/63/63646/HD_Data_Update_II_9-18-14.pdf, accessed September 14, 2015.

[3] *The Home Depot Reports Findings in Payment Data Breach Investigation*, November 6, 2014. Available at https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf, accessed September 14, 2015.

[4] Brian Krebs, *Banks: Credit Card Breach at Home Depot*, Krebs on Security, September 2, 2014. Available at http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/, accessed September 14, 2015.

57 lawsuits were subsequently filed against the company by consumers and financial institutions.[5] In January 2015, the district court for the Northern District of Georgia created separate tracks for the consumer and financial institution cases, noting that they "present[ed] significant, distinct factual and legal issues."[6] Consumers[7] and financial institutions[8] subsequently filed separate consolidated class action lawsuits.

Much has been written about consumer lawsuits stemming from data breaches.[9] Notably, however, there has been little discussion of litigation brought by financial institutions, despite the fact that such institutions have filed separate class action lawsuits in several major data breach cases, including *Home Depot*, *Target*, *Kmart*, *Mapco*, *Heartland Payment*, and *TJX*.[10]

Although questions remain as to how courts will analyze issues that arise in FI class action lawsuits, there are indications that these cases may be more likely to overcome threshold standing challenges than the consumer cases, and thus proceed to settlement or trial.[11] Therefore, it is important for companies whose systems have been breached to be aware that financial institution cases—in addition to those brought by consumers—are a real (and substantial) consequence of the breach. It is also important for all parties involved in data breach litigation to be prepared to develop economic models of harm to assist courts in determination of class certification, liability, and damages.

This article examines potential economic and legal issues in data breach litigation as they specifically relate to financial institution cases. Part II summarizes the types of harms typically claimed by FI

---

[5] David Allison, *Financial institutions claim Home Depot breach caused 'billions of dollars' in fraud losses*, Atlanta Business Chronicle, May 27, 2015. Available at http://www.bizjournals.com/atlanta/news/2015/05/27/financial-institutions-claim-home-depot-breach.html, accessed September 14, 2015.

[6] Case Management Order No. 2, In re: The Home Depot, Inc., Customer Data Security Breach Litigation, No. 1:14-md-02583-TWT, at 1 (N. D. Ga. January 16, 2015).

[7] Consumer Plaintiffs' Consolidated Class Action Complaint, *In re: The Home Depot, Inc., Customer Data Security Breach Litigation*, No. 1:14-02583-TWT (N.D. Ga. filed May 1, 2015). ("Home Depot Consumer Plaintiffs' Complaint")

[8] Financial Institution Plaintiffs' Consolidated Class Action Complaint, *In re: The Home Depot, Inc., Customer Data Security Breach Litigation*, No. 1:14-02583-TWT (N.D. Ga. filed May 27, 2015). ("Home Depot Financial Institution Plaintiffs' Complaint").

[9] For example, Mathew J. Schwartz, *Why So Many Data Breach Lawsuits Fail*, BankInfoSecurity, May 11, 2015. Available at http://www.bankinfosecurity.com/data-breach-lawsuits-fail-a-8213/op-1, accessed September 14, 2015; Judy Selby, *No Data Misuse? No Standing for Data Breach Plaintiffs*, Law360, April 24, 2014. Available at http://www.law360.com/articles/529877/no-data-misuse-no-standing-for-data-breach-plaintiffs, accessed September 14, 2015.

[10] *In re: The Home Depot, Inc., Customer Data Security Breach Litigation*, No. 1:14-02583-TWT (N.D. Ga. filed May 27, 2015) ("Home Depot"); *In re: Target Corporation Customer Data Security Breach Litigation*, MDL No. 14-2522 (D. Minn. filed Aug. 1, 2014) ("Target"); *Governmental Employees Credit Union v. Kmart Corporation et al*, No. 1:15-cv-03354 (N.D. Ill. filed Apr. 15, 2015) ("Kmart"); *Winsouth Credit Union v. Mapco Express Inc. et al*, No. 3:14-cv-01573 (M.D. Tenn. filed Jul. 31, 2014) ("Mapco"); *In re: Heartland Payment Systems, Inc. Customer Data Security Breach Litigation*, No. 4:09-MD-2046 (S.D. Tex. filed Jun. 26, 2009) ("Heartland Payment"); *In re: TJX Companies Retail Security Breach Litigation*, No. 07-10162-WGY (D. Mass. filed Oct. 25, 2007) ("TJX").

[11] Notably, the *Target* FI class was certified on September 15, 2015. (*See* Order Granting Class Certification, *In re: Target Corp. Customer Data Security Litig.*, MDL No. 14-2522-PAM-JJK (D. Minn. Sept. 15, 2015), ("Target Class Cert. Order").)

plaintiffs in such cases. Part III focuses on characteristics of FI plaintiffs that have distinguished them from their consumer counterparts, specifically on the notion of legal standing. Part IV discusses an economic framework relevant to the evaluation of damages claims in FI cases, as well as highlights important considerations relating to economic analysis in the class action context.

II. THEORIES OF HARM FINANCIAL INSTITUTIONS HAVE PROPOSED IN DATA BREACH CASES

The FI plaintiffs in *Home Depot* put forth theories of harm that are generally similar to those presented in other commercial data breach cases.[12] That is, plaintiffs have alleged that the data breach forced them to take actions to mitigate the effects of fraudulent transactions and prevent future fraud. Specific types of alleged injuries included (i) cancelling and reissuing payment cards, (ii) changing or closing accounts, (iii) notifying customers of compromised cards, (iv) investigating claims of fraudulent activity, (v) refunding fraudulent charges, (vi) increased fraud monitoring, (vii) lost interest and transaction fees due to reduced card usage, and (viii) devaluation of debit and credit cards.[13]

Comparing the FI claims in cases like *Home Depot* to those made in the parallel consumer cases highlights key differences in the types of alleged injuries, despite the fact that both stem from the same data breach. For example, harms claimed by FI plaintiffs generally relate to costs associated with mitigating or preventing fraud, most notably cancelling and reissuing affected cards.[14] In contrast, injuries alleged by consumer plaintiffs generally relate more to an increase in the *future likelihood* of suffering fraudulent charges, or to the misuse of the disclosed personal information.[15] As we discuss below, such differences illustrate the need for separate legal and economic analyses, depending on the type of plaintiffs involved.[16]

III. DISTINGUISHING CHARACTERISTICS OF FINANCIAL INSTITUTION CASES

At present, a significant threshold legal issue confronting all data breach plaintiffs—including financial institutions—is *standing*, or violation of a legal rights that entitles judicial relief. A number of consumer lawsuits to date have been dismissed for a lack of standing, especially under the 2013 Supreme Court case *Clapper v. Amnesty International USA*.[17] Financial institution claims, however, have thus far been less susceptible to this jurisdictional hurdle.

---

[12] *See* cases cited *supra* note 10. Although some firms have alleged additional types of injury such as "damages to Financial Institutions' reputations and lost customers." (Mapco Complaint, ¶55.)

[13] Home Depot Financial Institution Plaintiffs' Complaint, ¶187.

[14] *Ibid*.

[15] Home Depot Consumer Plaintiffs' Complaint, ¶2.

[16] For example, as the *Target* court opined that "there is a fundamental difference between the injury claimed in the consumer cases […] in which the risk of future harm is a possibility that one's financial information might at some point in the future be misused, and the injuries the [financial institution] Plaintiffs allege to have suffered. Most importantly, this is not a case in which Plaintiffs have yet to suffer any harm." (Target Class Cert. Order, at 7.)

[17] 133 S. Ct. 1138 (2013).

Standing Requirements and *Clapper*

To demonstrate standing, plaintiffs must meet three requirements: (i) injury in fact, (ii) causation, and (iii) redressability.[18] For *injury in fact*, a plaintiff must demonstrate violation of a legally protected interest that is "concrete, particularized, and actual or imminent."[19] For *causation*, the injury must be "fairly traceable" to the defendant's actions.[20] For *redressability*, the plaintiff must show that the injury can be "redressable by a favorable ruling."[21]

In 2013, the Supreme Court decision in *Clapper* clarified the "injury in fact" prong of standing doctrine.[22] The plaintiffs in *Clapper* were a group of U.S. reporters, lawyers, activists, and workers whose clients included detainees associated with the September 11 attacks.[23] In arguing that they had standing, the *Clapper* plaintiffs alleged two types of injury: (i) a *future* injury involving the threat of surveillance, and (ii) *present* injury involving present preventative costs. The threatened injury claim involved an "objectively reasonable likelihood" that the plaintiffs' client communications would be intercepted in the future.[24] The present injury claim asserted that the threat of surveillance required the plaintiffs to take costly and burdensome measures to protect their client communications.[25]

In a 5–4 decision, the Supreme Court held that the *Clapper* plaintiffs lacked standing under both claims. First, the Court held that threatened injury must be "certainly impending" and that the plaintiffs' allegations were too speculative to meet this requirement.[26] Second, the Court denied the plaintiffs' present-injury claims because the incurred expenses for which they sought remuneration were not based on mitigating injury that was "certainly impending."[27] Since 2013, lower courts have read *Clapper* as the governing standard for injury allegations involving uncertainty,[28] such as those typically claimed by plaintiffs in data breach class actions.

---

[18] *See* Article III of the U.S. Constitution.
[19] 133 S. Ct. 1138 (2013), at 1147 (internal quotation marks omitted).
[20] *Ibid*.
[21] *Ibid*.
[22] *Ibid*. *Clapper* involved a constitutional challenge to § 702 of the Foreign Intelligence Surveillance Act. Enacted in 2008, § 702 eased surveillance requirements for certain intelligence targets located abroad. (*See e.g.*, Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015). Available at http://www.harvard-jlpp.com/wp-content/uploads/2015/02/Donohue_Final.pdf, accessed September 14, 2015.)
[23] 133 S. Ct. 1138 (2013).
[24] *Id*. at 1146.
[25] *Id*. at 1146.
[26] *Id*. at 1147-48.
[27] *Id*. at 1151. Additionally, the Court acknowledged another standard for injury in fact based on a "substantial risk" of harm and "reasonably incur[red] costs" to mitigate or avoid that harm. However, the Court declared that the plaintiffs also failed under this standard. (*Id*. at 1150 n.5. *See also* Andrew C. Sand, *Standing Uncertainty: An Expected-Value Standard for Fear-Based Injury in Clapper v. Amnesty International USA*, 113 Mich. L. Rev. 711, 726-30 (2015) (arguing that footnote 5's "substantial risk" standard is distinct from the majority's "certainly impending" standard).)
[28] *See e.g.,* Amanda M. McDowell, *The Impact of Clapper v. Amnesty International USA on the Doctrine of Fear-Based Standing*, 49 Ga. L. Rev. 247, 260-64 (2014) (discussing treatment of *Clapper* by lower courts)

Consumer Claims Have Historically Struggled to Overcome Standing Hurdles

In data breach litigation, courts have been divided on whether consumer class action plaintiffs have standing to sue under *Clapper*, with some courts interpreting *Clapper* as imposing a high bar for injury claims by consumers, while others reading it more narrowly to allow standing for consumer plaintiffs.

On one side, federal courts in New Jersey,[29] Illinois,[30] Ohio,[31] Texas,[32] and the District of Columbia[33] have construed *Clapper* to require dismissal of consumer class action lawsuits. Oftentimes, these courts have found that consumer allegations of increased risk of harm and mitigation costs fall short of *Clapper*'s requirement for injury in fact. For example, *SAIC* provides one illustration of how courts have applied *Clapper* to deny consumer claims in data breach litigation.[34] The district court in *SAIC* rejected the vast majority of plaintiffs' claims for lack of standing. Relying on *Clapper*, the *SAIC* court declared that, "increased risk of harm alone does not confer standing"[35] and rejected the plaintiffs' claims of increased risk of identity theft and associated costs as insufficient for injury in fact.[36] The *SAIC* court also dismissed the plaintiffs' claims of actual misuse of personal information because there was insufficient "causal connection" to the defendant's actions.[37]

In contrast, federal courts in California[38] and Illinois[39] have interpreted *Clapper* narrowly to confer standing on consumer class action plaintiffs.[40] For example, in *Neiman Marcus*,[41] the district court dismissed the plaintiffs for lack of standing.[42] However, the Seventh Circuit reversed the decision,

---

[29] *See e.g.*, *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, No. CIV.A. 13-7418 CCC, 2015 WL 1472483 (D.N.J. Mar. 31, 2015); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451 (D.N.J. Dec. 26, 2013).

[30] *See e.g.*, *Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-CV-4787, 2014 WL 7005097 (N.D. Ill. Dec. 10, 2014); *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871 (N.D. Ill. Mar. 12, 2014); *In re: Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, (N.D. Ill. Sept. 3, 2013).

[31] *See e.g.*, *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio Feb. 10, 2014).

[32] *See e.g.*, *Peters v. St. Joseph Servs. Corp.*, No. 4:14-CV-2872, 2015 WL 589561 (S.D. Tex. Feb. 11, 2015).

[33] *See e.g.*, *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. May 9, 2014).

[34] *Id.*, at 1. In this case, consumers brought a class action lawsuit after the alleged physical theft of tapes that contained the personal information and medical records of approximately 4.7 million individuals.

[35] *Id.*, at 14.

[36] *Id.*, at 9-17.

[37] SAIC, at 22.

[38] *See e.g.*, *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sep. 4, 2014); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. Jan. 21, 2014).

[39] *See e.g.*, *Remijas v. Neiman Marcus*, No. 14-3122, 6-10 (7th Cir. 2015); *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014).

[40] A motion to dismiss was also denied on Article III standing grounds in *Corona v. Sony Pictures Entertainment*, No. 2:14-cv-09600-RGK-E (C.D. Cal. 2014). We do not discuss that case here due to Edgeworth Economics' involvement in the matter and the protective order entered therein.

[41] In this case, consumers brought a class action lawsuit after hackers potentially acquired the personal and financial information of approximately 350,000 cardholders. (*See* Paul A. Ferrillo, *Court: Neiman Marcus customers have standing to bring putative class action over data breach*, Cyber Risk Network, July 28, 2015. Available at http://www.cyberrisknetwork.com/2015/07/28/court-neiman-marcus-customers-have-standing-to-bring-putative-class-action-over-data-breach/, accessed September 14, 2015.)

[42] *Remijas v. Neiman Marcus*, No. 14-3122, 6-10 (7th Cir. 2015)

expressly holding that the plaintiffs' claims of increased risk of future fraudulent charges and greater susceptibility to identity theft met *Clapper*'s "substantial risk" requirement.[43] As a result, the *Neiman Marcus* court held that the plaintiffs' present injury claims of mitigation expenses passed *Clapper* and "easily qualifie[d] as concrete injury."[44]

The judicial divide in interpreting *Clapper* continues to inform the mixed treatment of consumer class action lawsuits. Thus, for many consumer plaintiffs, demonstrating standing has historically been uncertain and posed a substantial obstacle in data breach litigation.[45]

C. Financial Institution Claims Have Generally Not Faced Standing Challenges and Have Proceeded to Class Certification

Although consumer lawsuits have historically faced significant hurdles in terms of standing, financial institution cases have begun forging a different path. While the case law involving financial institutions is limited—most lawsuits are either ongoing or have settled[46]—to date, no federal court has dismissed a financial institution lawsuit arising from a major data breach for lack of standing.[47] Consider the ruling in *Target*, a case that relates to the alleged late-2013 theft by hackers of financial and personal information of approximately 110 million customers.[48] The court separated that litigation into consumer and financial institution cases,[49] and the defendant moved to dismiss both complaints. Notably, Target did not challenge the financial institutions' claims on standing grounds,[50] and in

---

[43] *Ibid.* ("At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach.") Furthermore, the Seventh Circuit distinguished *Neiman Marcus*, in which occurrence of the breach was not disputed, from *Clapper*, in which the speculative harm might not have affected all of the respective plaintiffs. (*Id*., at 10-11.)

[44] *Id*., at 10-11.

[45] Notably, however, the Third Circuit permitted the Federal Trade Commission to pursue administrative actions against companies that fail to protect consumer data. *FTC v. Wyndham Worldwide Corporation*, No. 14-3514 (3d Cir. Aug. 24, 2015).

[46] The data breach litigation for Target, Home Depot, Kmart, Mapco, and Heartland Payment are ongoing. The various financial institutions in TJX settled in 2007 through 2009. (Mike Cherney, *TJX Cos., Banks Settle Class Action Over Data Breach*, Law360, September 2, 2009. Available at http://www.law360.com/articles/120358/tjx-cos-banks-settle-class-action-over-data-breach, accessed September 14, 2015.)

[47] It is important to note two points regarding financial institution class action lawsuits in data breach litigation. First, to our knowledge, no court has explicitly applied *Clapper* to a financial institution class action lawsuit, although several cases have occurred post-*Clapper*. Second, several financial institution lawsuits have been dismissed on grounds other than standing, e.g., *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 164 (3d Cir. 2008).

[48] Chris Isidore, *Target: Hacking hit up to 110 million customers*, CNN, January 11, 2014. Available at http://money.cnn.com/2014/01/10/news/companies/target-hacking/, accessed September 14, 2015.

[49] Pretrial Order #1, *In re: Target Corporation Customer Data Security Breach Litigation*, (filed Sep. 2, 2014) (No. 14-2522).

[50] Defendant's Memorandum of Law in Support of Motion to Dismiss the Consolidated Class Action Complaint, *In re: Target Corporation Customer Data Security Breach Litigation*, (filed Sep. 2, 2014) (No. 14-2522).

December 2014, the district court ruled that the majority of the financial institutions' claims survived the motion to dismiss.[51]

While the financial institution cases may not get as much coverage in the press as their consumer counterparts, based on their relatively greater success (to date) at the early stage of litigation, they might be just as—if not more—important for breached firms in terms of legal exposure. Specifically, the particular injury claims in those cases (e.g., costs relating to cancellation and reissuance of affected cards) may lend themselves better to meeting standing requirements for injury in fact and causation than do the types of claims made by consumer plaintiffs.[52] While the facts and claims in a specific case are paramount in the evaluation of that case, the trend of defendants in FI data breach matters generally choosing to forgo standing challenges may indicate that the parties should be prepared to conduct a rigorous analysis of class certification issues.

IV. ECONOMIC ANALYSIS OF CLASS CERTIFICATION AND DAMAGES ISSUES IN FINANCIAL INSTITUTION CASES

As financial institution cases arising from data breaches proceed past the assessment of standing, courts will next focus on making an evaluation as to whether the proposed classes can be appropriately certified under Rule 23 of the Federal Rules of Civil Procedure. Among other issues, courts will be evaluating whether "questions of law or fact common to class members predominate over any questions affecting only individual members"[53] in these proceedings.

Economic analysis is an important component of many types of class actions and likely will gain similar prominence in data breach matters as those cases increasingly proceed to the class certification

---

[51] Memorandum and Order, *In re: Target Corporation Customer Data Security Breach Litigation*, No. 14-2522, at 1 (D. Minn. Dec. 2, 2014). The district court's opinion did not explicitly address standing, but by allowing the financial institutions to proceed past the motion-to-dismiss stage, standing was implied. This is because when hearing a case, a federal court must ensure that there is subject matter jurisdiction, which includes meeting the requirements of standing. 5B Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 1350 (3d ed. 1998) (discussing how federal courts at every level have an obligation to police subject matter jurisdiction).
Notably, the *Target* court opined that that "[a]lthough each member of the Plaintiff class must of course have standing to pursue its claims—that is, must have suffered an injury in fact that is capable of redress by a favorable decision—that every financial institution whose customers' cards were stolen in the breach suffered an injury in fact is readily apparent." (Target Class Cert. Order, at 11.) It is important to note, however, that the *Target* court did not apply *Clapper* in either case.

[52] As a general matter, in terms of injury, courts may find the claim of replacing affected cards to be more concrete than the typical consumer claim of increased risk, such as those dismissed in *SAIC*. Similarly, it may be that courts believe the replacement of affected cards bears a stronger "causal connection" to the defendant's actions than typical consumer claims of actual fraud, such as those also rejected in *SAIC*. (*See* discussion *infra* Section 0.)

[53] Rule 23(b)(3), Federal Rules of Civil Procedure.

stage.[54] This type of analysis assists the court in understanding the evidence and provides objective, independent testimony on the economic impact of the alleged conduct.

Economic experts are frequently employed in at least three phases of a class action, including class certification, liability, and damages. In the *class certification* phase, plaintiffs have the burden of proving by preponderance of the evidence that the same "common methodology" can be used to demonstrate that each potential class member was harmed by the alleged conduct and that the damages calculation reflects the liability theory.[55] At this stage, the economic expert provides testimony regarding the nature of the information and whether it can be applied to all class members collectively or, instead, must be considered on an individualized basis. In this section, we discuss an economic framework for evaluation of damages claims in financial institution cases, as well as highlight important considerations relating to economic analysis in the class action context.

A. Framework for Economic Analysis of Class Certification Issues

A primary role of an economic expert in a class action proceeding is to analyze whether the empirical evidence can be used to show the proposed class is cohesive enough to justify proceeding under Rule 23.[56] The purpose of the expert's assessment at this stage is to evaluate the proposed theories of harm in the context of the composition of the proposed class. That is, given class members' characteristics, is it in fact the case that all (or, in some cases, virtually all) could have suffered injury from the alleged conduct? Or, to the contrary, could (or did) some members avoid injury? Furthermore, can the expert determine injury using evidence common to the class, or will individualized inquires be necessary?[57] Similar questions with respect to damages must also be addressed by the expert at this stage. That is, the expert must evaluate whether a class-wide model can measure damages attributable to just the proposed theories of harm. If it cannot, the class action mechanism will not fit the facts of the specific case.

The answers to these questions are case-specific and ultimately serve as guidance for the court as to whether the proposed class should be certified and the litigation should proceed. However, there is substantial precedent from class actions in other areas (*e.g.*, *Comcast v. Behrend* in antitrust, *Wal-Mart v. Dukes* in employment, *Brazil v. Dole Food Company* in false claims, among many others) which dictates a rigorous expert review of these issues at the class certification stage. As data breach cases proceed to (and beyond) this stage, equally rigorous expert analyses will be required in order to help the court make an appropriate determination.

---

[54] Michael Kheyfets, *Beyond Standing: Economic Analysis of Class Certification Issues in Data Breach Class Actions*, Law360, May 14, 2015. Available at http://www.law360.com/articles/653885/beyond-standing-economic-experts-in-breach-class-actions, accessed September 14, 2015.

[55] Rule 23(a), Federal Rules of Civil Procedure.

[56] *See* note 54, *supra*.

[57] A rigorous analysis of the relationship between common and individual issues is essential from the perspective of the expert economist.

Economic analysis–particularly, the counterfactual paradigm–provides a rigorous framework to examine potential class certification and damages issues.[58] The framework compares the plaintiff's financial position in the "but-for world" where the breach did not occur to that in the "actual world" where it did.[59] The resulting differential forms the basis for damages claims. Importantly, however, while economic experts assume the allegations as true for the purposes of such analysis, it is *inappropriate to assume* that the conduct similarly affected all class members, or that a given model is applicable on a class-wide basis. The testing (and "falsifiability") of such assumptions forms the basis of economic science and must be implemented as part of the rigorous analysis of the claims.

To recreate the "but-for world" in a data breach case, it is necessary to evaluate whether any alleged economic harm to plaintiffs resulted from the data breach, or whether other factors unrelated to the breach may have also been relevant. If a putative class member is determined to be worse-off in the actual world than in the but-for world, that difference would the economic harm attributable to the data breach at issue. The goal of such analysis is to make each plaintiff whole to the extent there was economic harm resulting from the breach itself.

B. Economic Analysis of Claims in Financial Institution Cases

Above, we have described specific types of economic injuries alleged in *Home Depot* and other financial institution cases.[60] The variety of claims, the sizes of the proposed classes,[61] and the "massive"[62] sizes of the financial damages claims in these cases all underscore the importance of rigorous economic analysis at the class certification stage. That is, when a proposed class is made up of thousands of financial institutions—with each individual entity harmed in a number of ways—the certification of that class rests crucially on the plaintiffs' ability to design a model capable of determining whether all (or, in some cases, virtually all) class members could have suffered injury from the alleged data breach.

Ultimately, the plaintiffs' burden is to propose a method that would be able to evaluate whether a particular type of claimed harm (as well as all the other proposed types of harm) from the alleged data breach can be evaluated on a class-wide basis. If the method is unable to do so for all (or virtually all) class members, certification of the proposed class may not be appropriate. To illustrate the relevant economic considerations in financial institution cases, this section examines three claims generally alleged in such cases (including by the *Home Depot* plaintiffs): (i) costs associated with cancelling and

---

[58] Matthew Milner, *The Role of Economics in Data Breach Class Actions*, Law360, September 19, 2014. Available at http://www.law360.com/articles/578387/the-role-of-economics-in-data-breach-class-actions, accessed September 14, 2015.
[59] *Id*.
[60] *See* Section II.
[61] For example, the *Home Depot* plaintiffs have alleged a class of "more than 5,000 members in the FI National Class." (Home Depot Financial Institution Plaintiffs' Complaint, ¶198.)
[62] *Id.*, ¶188.

reissuing affected payment cards, (ii) investigating claims of fraudulent activity and refunding fraudulent charges, and (iii) lost interest and transaction fees due to reduced card usage.[63]

1. Valuation of Card Reissuance Costs in a Class Action Context

A typical claim made in several FI cases is that as a result of a data breach, financial institutions were forced to incur the cost of cancelling and reissuing payment cards that they would not otherwise have had to.[64] For example, *Home Depot* plaintiffs stated that (i) the Credit Union National Association "estimated that 7.2 million cards issued by credit unions were compromised, that credit unions incurred $60 million in reissuance costs, and that the approximate replacement cost per card was $8.02," and (ii) Independent Community Bankers of America "estimated that community banks were forced to reissue nearly 7.5 million cards at a cost of more than $90 million."[65]

Assessing this kind of claim on a class-wide basis, however, can raise certain issues. For example, while calculating *aggregate* reissuance damages can appear to be a seemingly simple arithmetic exercise (i.e., multiplication of "cost per card" by the number of "cards issued"), average or aggregated metrics may mask issues specific to individual financial institutions. That is, determining the actual number of cards needing to be replaced *as a result of the data breach* (as opposed to, for example, ordinary expiration) may be an important source of variation across class members. Similarly, it may be the case that no single cost metric is representative of the class. Larger financial institutions may have economies of scale with respect to card replacement relative to smaller ones,[66] and may also choose to replace a relatively smaller portion of cards in circulation.[67]

Importantly, financial institutions may also respond differently to a given data breach, rendering the assumption of a uniform card reissuance cost model problematic. For example, some class members may choose to reissue both credit and debit cards, others may choose just one or the other, while others still may choose "active monitoring" in lieu of a mass reissuance.[68]

---

[63] *Id.*, ¶187.
[64] *Id.*, ¶187.
[65] *Id*. at ¶189. *Home Depot* plaintiffs further stated that "because credit unions and community banks issued only a portion of the cards that were compromised by the breach, the total reissuance costs incurred by all financial institutions is much higher."
[66] American Bankers Association Target Breach Impact Survey, July 2014, p. 11. Available at http://www.aba.com/Tools/Function/Payments/Documents/TargetBreachBankImpact.pdf, accessed September 14, 2015.
[67] *Id.*, p. 7.
[68] *Large Financial Institutions Choose Mass Card Reissues in Wake of Target Breach*, February 2014. Available at http://www.firstannapolis.com/articles/large-financial-institutions-choose-mass-card-reissues-in-wake-of-target-breach, accessed September 14, 2015.

Additionally, the issue of causality will be important to any economic model proposed for measuring reissuance cost damages.[69] Given the prevalence of payment card data breaches, such a model would need to specifically tie the damages estimate to the breach at issue, as opposed to other causal factors such as concurrent breaches at other companies, market forces, or internal considerations (such as a pre-established plan to replace the cards).[70] For example, there were at least a dozen other payment card data breaches around the time of the Target event in late 2013.[71] A rigorous economic analysis would have to examine whether there are other plausible motivations for replacing cards and how those vary across putative class members. To the extent other causal factors exist—e.g., cards issued by a given financial institution were disclosed in multiple breaches—the simple arithmetic approach described above may be inadequate as a class-wide method.

2. Valuation of Fraudulent Charges Costs in a Class Action Context

As with reissuance costs, using aggregate metrics to model harm from fraudulent charges may be a tempting but potentially problematic approach to economic evaluation of class certification and damages issues. For example, *Home Depot* plaintiffs stated that "based on prior thefts of customer information, credit card firm BillGuard predicts that an average of $332 in fraudulent charges will be made on each card used by the thieves and that the total fraud losses will approximate $3 billion"[72]

Such "simple math" of calculating class-wide fraud damages by multiplying an estimated amount of per-card fraud by the number of cards with fraudulent activity may also mask important variation across class members. For example, the number of affected cards may vary widely by class member (i.e., this is an empirical question and it cannot be assumed, for example, that the number of affected cards is proportional to the financial institution's size[73]). Similarly, the magnitude of fraudulent charges may vary as well,[74] with many cards potentially suffering *no fraudulent charges at all*. If variation in these metrics across financial institutions exists, a single average model may not be representative of some (or many) of the class members' experiences.

Lastly, economic models plaintiffs put forth for the purposes of class certification or damages must consider the "but-for" levels of fraudulent activity. That is, because fraudulent activity would likely take place even in the absence of any single data breach, the model would need to determine—for a

[69] Under the standard established in the Supreme Court's decision in *Comcast Corp. v. Behrend*, at the class-certification stage, a plaintiff must provide a reliable damages model which specifically measures only the damages or harm attributable to the plaintiff's particular theory of liability. (*Comcast Corp. v. Behrend*, 133 S. Ct. 1426 (2013))

[70] Decision and Order on Plaintiffs' Revised and Supplemented Motion for Class Certification, *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, No. 2:08-md-1954-DBH, at 20-23 (D. Me. Mar. 20, 2013).

[71] *See* http://www.privacyrights.org/.

[72] Home Depot Financial Institution Plaintiffs' Complaint, ¶190.

[73] *See e.g.*, American Bankers Association Target Breach Impact Survey, July 2014, p. 9.

[74] For example, in the Target consumer case, individual consumers claimed fraudulent charges that ranged in amount from $100 to several thousands. (Consumer Plaintiffs' First Amended Consolidated Class Action Complaint, *In re: Target Corporation Customer Data Security Breach Litigation*, MDL No. 14-2522 (D. Minn. Filed Dec. 1, 2014), ¶1.)

given financial institution—the *incremental* increase in fraud level *resulting* from the breach. Similar issues may arise here as well, since (i) aggregate historical or predicted future levels of fraud may not be valid class-wide benchmarks, (ii) industry-wide levels of fraud may not be representative for any given FI, (iii) there may be no way to determine whether incremental changes are due to the breach at issue or any number of other breaches, and (iv) many other factors (e.g., level of credit card activity) may affect fraud costs.

3. Valuation of Lost Fees in a Class Action Context

Home Depot plaintiffs, like those in several other financial institution cases, alleged damages for "lost interest and transaction fees due to reduced card usage resulting from the breach."[75] As with the other theories of harm, rigorous analysis would be required to capture the nuances of the world that would have existed but for the data breach. For example, the damages model would need to be able to capture the "chilling" effect (if any) on levels of payment card usage resulting specifically from the alleged breach.[76] Similarly, to the extent such changes in usage varied between class members, any average model may not yield results that are useful across the proposed class.[77]

In addition to the change in the *number* of transactions as a result of a breach, the "lost fees" damages theory is also dependent on the *type* of transactions that customers forego after the breach. Interchange fees charged by issuer banks (i.e., the plaintiffs in financial institution cases) are highly complex and variable.[78] This means that even if consumers forego certain transactions, the fees lost by individual FIs may only be ascertainable by individualized inquiries into that FI's fee structure and the types of transactions that FI lost as a result of the breach.

---

[75] Home Depot Financial Institution Plaintiffs' Complaint, ¶221.

[76] For example, a CreditCards.com survey conducted in October 2014 found that 52 percent of responders "probably" or "definitely" would shop at a store that had a data breach, indicating that consumer response to breaches is variable. *See* Karen Haywood Queen, *Poll: Nearly half of cardholders likely to avoid stores hit by data breaches*, CreditCards.com, October 19, 2014. Available at http://www.creditcards.com/credit-card-news/shopping-after-breach.php , accessed September 14, 2015. (*See also* "Target data breach: Poll finds shoppers doing little in response," January 27, 2014. Available at http://www.oregonlive.com/business/index.ssf/2014/01/target_data_breach_poll_finds.html, accessed September 14, 2015.)

[77] In an extreme example, if one FI's customers ceased using their cards entirely after a breach, and another's did not change their card usage behavior at all, the "lost fees" harm caused to the two FIs by the breach would vary by 100 percentage points and would not be adequately represented by an average (i.e., 50 percent lost fees for each FI).

[78] *See e.g.*, Visa USA Interchange Reimbursement Fees, October 18, 2014. Available at http://www.merchantid.com/pdfs/Visa-USA-Interchange-Reimbursement-Fees-2014-Oct-18%202%20-%20Visa-USA-Interchange-Reimbursement-Fees-2014-Oct-18.pdf , accessed September 14, 2015.

V. CONCLUSION

The ubiquity of class action cases filed against businesses suffering data breaches (as well as the speed with which they are filed after the breach is announced) is indicative of plaintiffs' view that the class action mechanism is best suited to litigating data breach cases. As these cases have evolved, however, a distinction has arisen between consumer and financial institution matters. The former involves customers of the breached party, whose information was stored as a result of transactions the parties engaged in and whose theories of harm generally pertain to out-of-pocket costs and increased risk of identity theft. The latter generally involves banks who issued credit cards those customers used, and who claim damages relating to the reissuance of cards, costs associated with fraudulent charges, and lost fees (among others).

While the jurisprudence with respect to both types of cases continues to evolve, to date, financial institution cases have had more success proceeding past court's evaluations of standing. As a result, both because courts have indicated that FI cases merit separate consideration and because those cases may be more likely to proceed, it is important to develop economic frameworks that specifically evaluate injuries claimed by financial institutions. Given the potential financial exposure at stake in these matters, as well as the sizes and variability of the proposed financial institution classes, a counterfactual framework—based on rigorous economic analysis—is critical for analyzing claims like the ones made by plaintiffs in Target, Home Depot, and others.

Michael Kheyfets *is a Partner at Edgeworth Economics. As part of Edgeworth's Privacy and Data Security practice, Michael works with clients and outside counsel on economic issues related to data privacy and data security claims. He applies his expertise in rigorous empirical analysis to assisting clients with answering complex questions surrounding the assessment of potential financial exposure from a claim. He also applies his extensive experience in analyzing large data sets as well as developing and validating a variety of models to empirically analyze issues of class certification and damages. Michael received his B.A., magna cum laude and Phi Beta Kappa honors, and his M.A. in economics from Boston University. He currently serves as a Young Economist Representative on the American Bar Association's Section of Antitrust Law Economics Committee and holds a CIPP-US (Certified Information Privacy Professional, US private-sector) certification from the International Association of Privacy Professionals*.

Matthew Milner *is a Partner and Co-founder at Edgeworth Economics and chairs the firm's Privacy and Data Security practice. In cases involving data breaches, Matthew works with businesses and counsel to identify and analyze data systems to assess exposure and potential damages. He works with clients to understand the relationships between databases and how the data can be used to determine the size of the breach, quantify the number of potentially impacted records, and identify where those account holders are located. Matthew received his M.B.A. from The George Washington University School of Business and his B.A. in Economics and Political Science from Hobart College. He holds a CIPM (Certified Information Privacy Manager) certification from the International Association of Privacy Professionals.*

Andrew Sand *is a judicial clerk to the Honorable Michael S. Kanne, United States Court of Appeals for the Seventh Circuit. Prior to his current role, Andrew worked at Edgeworth Economics, assisting with legal issues and economic analysis in a number of matters. He has previously written on standing in the Michigan Law Review and has significant experience creating complex empirical models and analyzing large datasets in various academic and professional settings. Andrew holds a J.D. from the University of Michigan Law School, where he was an editor for the Michigan Law Review. Additionally, he holds an M.S. in Statistics and B.A. in History from Stanford University. The views expressed here represent those of the author in his private capacity and do not in any way represent the views of the court or any other entity of the United States Government.*