MINTZ

Precedent and the Price Explain Why Target and the Consumer Class Agreed to an Early Data Breach Settlement

March 20, 2015 | Blog | By **Kevin M. McGinty**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

On March 18, 2015 – **just three months after denial of a motion to dismiss consumer claims arising from Target's 2013 data breach** – Target and the consumer class filed papers seeking approval of a settlement. The proposed **settlement agreement** creates a $10 million cash fund to be paid out to class members claiming actual damages arising from the settlement. Settlement funds will be distributed in a claims-made process to be run by a settlement administrator (the cost of which will be borne by Target). The maximum claim amount is $10,000. Claims without supporting documentation are capped at lower dollar amounts. Unclaimed funds will not revert to Target, but will be redistributed to class members submitting claims or as otherwise directed by the Court. The settlement also calls for non-cash relief consisting of the adoption of certain data security protection practices and appointment of a chief information security officer. Finally, class counsel have indicated that they will apply for $6.75 million in attorneys' fees.

Why the quick settlement? Settlements in prior data breach cases provide a clue. Even where cases survive motions to dismiss, obstacles to proving consumer damages on a classwide basis drive down the cost of settlement. Most consumers are not required to pay for fraudulent charges made on credit or debit cards. Retailers often provide free credit monitoring services to mitigate any risk of credit impairment or identity theft. Few consumers suffer catastrophic harms and, when they do, their injuries are not susceptible to proof through evidence common to the class as a whole. As a result, consumer settlements in data breach class actions offer relatively small compensation in relation to the size of affected classes.

How small? In a submission intended to show the reasonableness of the proposed Target settlement, the consumer plaintiffs provide **chart** listing prior settlements on behalf of consumer classes in data breach cases. The cash settlements in the largest cases are highly illuminating:

- • *In re Countrywide Fin. Corp. Customer Data Security Breach Litig.* (mortgage lender): Settlement fund of $6.5 million to settle claims of over 17 million class members.
- • *In re TJX Cos. Retail Security Breach Litig.* (retailer): Claims made settlement fund of $10 million to resolve claims of almost 46 million TJX customers.
- • *In re Sony Gaming Network and Consumer Data Security Breach Litig.* (online gaming network): Settlement fund consisting of $1 million in cash plus $14 million in non-cash benefit to settle claims of about 24.6 million class members.
- • *In re Department of Veterans Affairs (VA) Data Theft Litig.* (federal agency): $20 million settlement fund to resolve claims of class of 26.5 million patients whose data was compromised.
- • *In re LinkedIn User Privacy Litig.* (online social networking site): Settlement fund of $1.25 million to defray expenses, incentive awards and claims in connection with class of about 800,000 users.

As these settlements illustrate, the cash cost of a large data breach settlement is typically $1.00 or less per class member, and none involving non-medical records provided aggregate cash payments in excess of $10 million. Given that price range for consumer data breach settlements, Target's choice to settle promptly was likely an easy one. Here, Target will be paying $10 million in cash to resolve the claims of an estimated 110 million class members, a per-class member amount that is well below the settlements in other consumer cases. The settlement makes even more sense when weighed against the cost of ongoing litigation and the overall cost of responding to the data breach. Assuming a total settlement cost of $20 million – consisting of cash, plaintiffs' counsel fees, ongoing defense attorneys' fees and settlement administration costs – that amount still pales in comparison to the **$252 million that Target has expended to date in responding to the data breach**. The ability to settle the consumer claims cheaply means that incurring additional litigation expenses – and likely ending up in the same place –

would make little sense.

The court **issued an order on March 19** that preliminarily approved the settlement, approved the proposed class notice, and set the schedule for opt-outs, objections and final approval of the settlement. Class members will have until July 31 to opt out of the class or to submit objections. (If 5,000 or more class members opt out, Target will have the right to terminate the settlement). The final approval hearing is set for November 5, 2015.

The pending settlement does not cover the claims of the card issuer class, **which seeks recovery of amounts paid out for fraudulent charges against credit and debit cards compromised in the breach**. The claimed damages for the card issuers are likely to dwarf those recoverable by consumers because the issuers, unlike the consumers, bore the brunt of fraudulent charges made using stolen payment card information. While at least one commentator has suggested that **the promptness of the consumer settlement provides some hint as to the strength of card issuers' claim that Target is culpable for failing to prevent the breach**, the economic considerations outlined above provide more than sufficient justification for the settlement without regard to the strength or weakness of Target's defense on the merits. Because the probable size of the card issuers' claims will provide ample incentive for Target to continue to pursue an expensive defense on the merits, it may not be possible to assess the strength of such a defense until further discovery and motion practice in the case plays out. For now, the proposed consumer settlement allows Target to fight a single-front war, devoting all of its energies to responding to the card issuer claims.

Authors

Kevin M. McGinty, Member / Co-chair, Class Action Practice

Kevin is a member of the firm's Health Care Enforcement Defense Group and has significant experience representing health care–related entities in a variety of litigation matters, including contract, regulatory, False Claims Act and class action lawsuits. Kevin's health care industry clients have included pharmacies, PBMs, hospitals, clinical laboratories, diagnostic imaging providers, pharmaceutical companies and managed care organizations.