WEBINAR

# Handling Data Breach Class Actions

Thursday, March 21, 2024


**Anjali Das**
Partner - Chicago, IL
312.821.6164
anjali.das@wilsonelser.com

**David Ross**
Partner - Washington, DC
202.626.7687
david.ross@wilsonelser.com


WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP


1

## Overview: Data Breach Class Actions

- Complaints (allegations and damages)
- State v. Federal Court
- Motion to Dismiss
  - Article III standing (Rule 12(b)(1))
  - Failure to state a claim (Rule 12(b)(6))
- Class Certification
- Settlements
  - Claims-made versus common fund
- Challenges due to influx of plaintiffs' firms filing suits
- Key considerations for defense and settlement




2

## 2023 Data Breach Class Action Statistics

- 1320 suits filed in 2023 (versus 604 in 2022)
- Includes copy-cat suits across multiple jurisdictions
- Rise in cases attributed to various factors
  - Shift to remote workforce
  - Rise of cloud-based storage
  - Geo-political landscape
  - Escalation of sophisticated cybercriminal activity
  - Third party data breaches
- MOVEit cases
  - 100+ class actions in MDL proceeding in Massachusetts
  - Russian cybergang's exploitation of vulnerability in file transfer software
  - Suits name Progress Software (MOVEit developer) and customers/victims




3

## Cyber Attack on Change Healthcare

- Change Healthcare processes 15B healthcare transactions each year
- Incident has disrupted healthcare and patient billing nationwide
- Unprecedented magnitude of CH cybersecurity incident
  - CH Blackcat ransomware attack
  - Theft of 6 TB of data
  - $22M ransom
- "Incident is a reminder of the interconnectedness of the domestic healthcare ecosystem" (HHS)
- Providers facing significant cash flow problems as a result
- HHS investigation
- Class Actions are piling up




4

## Data Breaches = Class Actions

- Suits filed on the heels of (public) notice of data breach
  - "Rush to the courthouse" within weeks or months
  - HHS "Wall of Shame," AG websites, posting on company websites
- Plaintiff's firms that specialize in data breach class actions
- Ambulance chasing:  FB and social media posts
- Multiple complaints filed in state and/or federal courts
- Easy to file, not always so easy to defend
- Parallel regulatory investigations


5

5

## Data Breach Class Actions
## Typical Allegations

- Suit filed by named plaintiff(s) on behalf of proposed class
- Class = notice population (customers, patients, employees)
- Defendant failed to properly safeguard plaintiff's PII/PHI
- De facto "strict liability" for not preventing breach
- Despite common knowledge that cyberattacks are prevalent
- Failure to comply with HIPAA, FTC or other industry standards
- Violation of defendant's privacy policy
- Insufficient or untimely notice of data breach
- Cybercriminals can sell, leak, or otherwise misuse PII/PHI


6

6

## Change Healthcare Class Actions

- Growing number of class actions filed in federal courts against CH
- The next "Blackbaud" line of cases?
- Public notice of incident on CH website
- Plaintiffs are patients of CH or health providers that use CH platform
- Failure to implement adequate measures to safeguard PII/PHI
  - "laundry list" of cybersecurity measures (e.g., encryption, etc.)
  - Violation of HIPAA and FTC Act and guidance
- Resulting in theft by cybercriminals
- Alleged injuries due to theft of PII/PHI (economic loss?)
- Myriad claims
  - negligence, negligence per se, breach of implied contract, unjust enrichment

 7

7

## Data Breach Class Actions
## Typical Alleged Injuries

- Fraudulent misuse of PII? (sometimes)
  - Fraudulent charges to account
  - Fraudulent accounts opened
  - Increased spam calls, text messages
- Unreimbursed expenses
  - Purchase of credit monitoring/ID theft
  - Expenses to cancel/replace payment cards
- Imminent risk of (future) harm or identity theft
- Diminished value of PII
- Lost time (risk mitigation efforts)
- Benefit-of-the-bargain damages (payment for data security)
- Anxiety, emotional distress


 8

8

## State v. Federal Court

| Federal Court | State Court |
|---|---|
| Article III Standing (concrete injury in fact) | State court standing tests are generally more liberal |
| Federal courts more inclined to grant a motion to dismiss a complaint at the pleading stage where warranted | State courts typically inclined to allow cases to proceed at pleading stage (trial courts) |
| Many more precedential federal data breach court opinions | State courts not bound by federal court opinions; might have limited (or no) binding state opinions |
| Federal courts more sophisticated, more experience with complex class actions | Greater need to educate state courts on data breach cases and underlying incidents |
| Rigorous Federal Rules of Civil Procedure that dictate all aspects of motion practice, discovery, deadlines, etc. | State courts generally more lax in terms of procedure; may allow discovery to proceed at outset of a case (discovery may be served with complaint) |
| Related cases filed in different federal courts can be consolidated or coordinated/consolidated in an MDL proceeding | State court actions cannot be consolidated unless they are in the same court; no mechanism to consolidate state and federal court actions (parallel proceedings) |
| Federal court may not have subject matter jurisdiction if 2/3 or more of proposed class members are citizens of the same state | Local counsel is often required to appear at all hearings |
| Class action settlements have rigorous court approval process | Some state courts are more closely scrutinizing claims-made settlements |




9

## Article III Standing Threshold Issue in Federal Court

Has plaintiff adequately alleged an injury in fact?

- Standing is an essential part of the case-or-controversy requirements of Article III of the U.S. Constitution and threshold issue of law
- To have standing, plaintiff must show each of the following:
  1) "injury in fact" that is concrete and particularized . . . not hypothetical;
  2) injury is fairly traceable to the challenged action of defendant; and
  3) it is likely that the injury will be redressable by a favorable decision by the court.
- Federal courts evaluate standing under Fed. R. Civ. P. 12(b)(1)
- Standing must exist even in the context of a suit for statutory violations
- Concrete injury may include physical, monetary or intangible harm




10

# Seminal Decisions on Standing

| Case | Overview | Ruling |
|---|---|---|
| ***TransUnion v. Ramirez*** (S.Ct. 2021) | Class action for violations of FCRA. Class members credit reports identified them as "terrorists." Some reports shared with 3P. | Risk of future harm alone is not enough to establish standing in a case for damages. Must be accompanied by some other present concrete harm. |
| ***Bohnak v. Marsh & McClennan*** (2d Cir. 2023) | Unauthorized access to PII by cybercriminals (including SSNs). No actual misuse of PII, identity theft or financial fraud. | **Standing**. Exposure of PII to "malevolent actor" constitutes a concrete harm AND plaintiffs also incurred lost time and expenses to mitigate risk of harm. |
| ***Clemens v. ExecuPharm*** (3d Cir. 2022) | CLOP ransomware attack. PII (including SSNs) was leaked on the Dark Web. No actual misuse of PII. | **Standing**. Targeted attack to steal PII which stolen and posted on the Dark Web. Type of PII could be used to commit ID theft. |
| ***Webb v. Injured Workers Pharmacy*** (1st Cir. 2023) | Cyber attack leading to unauthorized access of PII (including SSNs). One plaintiff experienced fraudulent tax return. Others alleged lost time and risk of future harm. | **Standing.** "Loss of time is equivalent to a monetary injury which is indisputably a concrete injury." |
| ***Green-Cooper v. Brinker International*** (11th Cir. 2023) | Credit card data breach. PCI posted online for sale. 2 plaintiffs experienced unauthorized credit card charges. All plaintiffs experienced lost time to remediate risk of harm. | **Standing** based on theft and posting of stolen credit card data (misuse). |

 

11

# Standing Factors To Consider

| Factor | Description | More likely to support standing |
|---|---|---|
| Nature of incident | Ransomware, BEC, inadvertent disclosure | Ransomware (intentional, targeted attack) |
| Type of PII | SSNs, DOB, DLN, financial information, health information | SSN most likely to result in risk of future harm of fraud or ID theft |
| Actual misuse of PII (versus risk of future harm alone) | Fraudulent tax returns, charges, accounts opened, etc. | Note: Theft and/or leaking of data by bad actor is also construed as misuse of PII |
| Lost time or expense | Lost time or expense mitigating risk of future harm (reviewing account statements, freezing credit, closing accounts, registering for ID theft protection services, etc.) | Lost time or expense coupled with compromise of SSN or actual misuse of PII |
| Anxiety | Anxiety related to risk of future harm | Anxiety alone should not create standing |
| Diminished value of PII | Theft of PII by cybercriminals has resulted in diminution in value of PII | This argument is not typically favored by courts |
| Benefit of bargain damages | Plaintiff allegedly paid for goods or services which included data protection | Courts split on whether this constitutes injury or harm |

 

12

## Practical Considerations in Defending Data Breach Cases

| Pros | Cons |
|---|---|
| Avoid waiving legal defenses (not realistic to forego filing a motion to dismiss and filing an answer instead) | Time and expense |
| Leverage for future settlement negotiations | Cannot file a "canned brief" since legal analysis is based on specific facts and circumstances (and jurisdiction) |
| Creating new (possibly favorable) case law (*e.g.*, NY Ct. App. decision in *Syracuse* class action) | Must cite any case law that is binding on the particular court and continuously update case law |
| Getting some of the causes of action dismissed such as statutory claims with statutory damages that could inflate the value of the case (*e.g.*, CMIA, CCPA, etc.) | Courts typically permit plaintiffs leave to file an amended complaint so may have to file a second motion to dismiss |
| Can always explore settlement and mediation pre, post, or pending ruling on motion to dismiss | Cannot file the same motion to dismiss in state and federal cases based on different legal thresholds for standing, etc. |
| Two "bites of the apple" in a MTD based on standing (Rule 12(b)(1) and failure to state a claim (Rule 12(b)(6); can also explore packaging with a Motion to Strike Class Allegations | If there are parallel state and federal court proceedings, a favorable ruling in one court does not mean an automatic dismissal of case in other court; motions to strike disfavored |
| Also consider filing Motion to Compel Arbitration if contract exists with mandatory arbitration and class action waiver provision. (Plaintiffs may choose to walk away from case) | Must accept the facts pled in the complaint as "true" – cannot contest factual accuracy of allegations on a MTD |




13

## Data Breach Class Actions Class Certification

- FRCP 23(a) (and state law equivalents)
  - Numerosity: Class is so numerous that it would be impracticable to join all class members
  - Commonality: Questions or law or fact common to the class
  - Typicality: Claims or defenses of class representative are typical for all class members
  - Adequacy: Class representation (and their counsel) will adequately protect the interests of the class
- FRCP 23(b)(3) (and state law equivalents)
  - Predominance: Issues of law or fact common to all class members "predominate" over individual issues (for cases seeking money damages) and class action is superior to other forms of adjudication




14

## Data Breach Class Actions Mediation

- Data breach class actions feature a high rate of settlements
- Individual v. class settlement
- Frequency of mediation as vehicle to class settlement
- Pre-mediation discovery – what to expect and how to respond
- Frequent disclosures in pre-mediation discovery
- Mediation – who participates from both sides and participation by insurer representatives




15

## Data Breach Class Actions Common Fund Settlements

- Low payouts in data breach class settlements:
  - Most class members ignore class notices as a matter of practice or due to receiving multiple class notices
  - Few class members have documented “out-of-pocket” losses to reimburse associated with the cyber incident
  - If “lost time” reimbursement requires associated “out-of-pocket” losses, these claims are also scant
  - Many class members have a conscience and will not claim “lost time” they did not actually expend, or do not want to take the effort to seek recovery of “lost time”
  - Most class members see little value in signing up for any, or additional, credit monitoring




16

## Data Breach Class Actions Common Fund Settlements

- Plaintiffs' counsel present "non-reversionary" common fund settlements as the "gold standard" to provide closure and certainty in the approval process (often with residual funds paid out to class members) – counsel often refuse to consider alternative structure for class settlement
- Claims-made settlements are not unachievable, but more difficult to obtain and need careful crafting. Hybrid class settlements could also be considered, with guaranteed payout benefits, such as pro rata case payouts to all or certain class members who submit a claim




17

## Growing and Crowded Field of Plaintiffs' Attorneys

Plaintiffs' attorneys and law firms are flocking to "get in on the action"

- Increase in cyber attacks and victims (more sensitive data, AI use)
- Third parties established to funnel plaintiffs to lawyers
- Increase in automation in tracking allows for faster retentions of plaintiffs
- Increase in companies with cyber coverage to respond to data breach class actions
- Ability to use template pleadings and filings to allow quicker entry into marketplace ("copy and paste" pleadings), and can team with other firms to litigate cases
- Opportunity to file class actions in different jurisdictions and in state or federal courts opens the doors to more law firms and increase in data security/privacy statutes enacted in states entice more filings
- Favorable recent "standing" and other rulings (TransUnion is not a "stone wall") and sizeable data breach class settlements with significant attorney's fees elements embolden more attorneys to get involved, with courts more sympathetic to plaintiffs and harm caused by data breaches




18

## Growing and Crowded Field of Plaintiffs' Attorneys

Challenges of more Plaintiffs' attorneys and law firms getting in on the action:

- Prior cases filed by same group of plaintiffs' lawyers allowed for better estimates of a "road map" the class action would likely follow, and the structure and amounts for a class settlement that could be achieved – more uncertainty
- Multiple filings or retentions of multiple plaintiffs by different law firms requires plaintiffs' attorneys to reach allocations of fees among several law firms, pushing up the amount of fees that will be sought and the potential "road map" of the case
- Plaintiffs' attorneys are in open competition. A "bad deal" settlement reached by plaintiffs' counsel could negatively influence the willingness of other plaintiffs' law firms to work with that counsel in other cases

 

19

## Growing and Crowded Field of Plaintiffs' Attorneys

Challenges of more Plaintiffs' attorneys and law firms getting in on the action:

- Some plaintiffs' law firms with experience in other types of class actions bring an expectation for hefty attorney's fees
- Presence of some favorable decisions allow cases to survive dismissal creates less leverage for filing a motion to dismiss
- Plaintiffs' attorneys may be willing to let cases proceed into discovery and beyond to try to extract a more robust settlement or "roll the dice" to try to achieve class certification
- The "remaining limits on the policy" approach to serve as a ceiling for any settlement is no longer as certain to resolve a case
- Experienced defense counsel may need to take more of a laboring oar in getting class settlements approved and processed

 

20

## Key Considerations for Data Breach Class Actions

- Dispositive motion practice is still a key strategy and may be enhanced with a motion to strike class allegations, but realistic expectations are necessary depending on the cases and venue – note that dark web posting often significant to courts to find harm
- Common funds must be anticipated for class settlements, but claims made and particularly hybrid structures should not be "off the table" and individual settlement angles should be examined
- For some cases, in person mediation may be more productive than a "Zoom" mediation
- Cases may need to be litigated through a motion for class certification (after discovery), as only a handful of data breach class cases have been certified and few proceed to that phase of the case – in 2023, 15% certification granted and 85% denied
- Case consolidation may need early consideration when multiple filings, even before dispositive motion practice or early mediation




21

## Thank you for attending!

**Anjali Das**
Partner, Cochair Cybersecurity & Data Privacy Practice
Chicago, IL
anjali.das@wilsonelser.com

**David Ross**
Partner
Washington, D.C.
david.ross@wilsonelser.com




22