MAYER·BROWN

Trends in Data Breach and Cybersecurity Regulation, Legislation and Litigation

April 17, 2014

MAYER·BROWN

“For nearly a decade, we’ve had major data breaches at companies both large and small. Millions of consumers have suffered the consequences….”

Sen. John D. Rockefeller, D-W.Va.

Chairman, Senate Committee on Commerce, Science and Transportation

Sponsor of Staff Report, “A ‘Kill Chain’ Analysis of the 2013 Target Data Breach”

MAYER·BROWN

In 2013, “the US … experienced the highest total average cost at more than $5.4 million [per data breach].”

Ponemon Institute LLC

2013 Cost of Data Breach Study: Global Analysis

Average per capita cost defined as cost of data breach divided by number of records lost or stolen

MAYER·BROWN

"The [FTC] has made it clear that it does not require perfect security, and the fact that a breach occurred does not mean that a company has broken the law."

Edith Ramirez
Chairwoman, Federal Trade Commission

Testimony before Senate Commerce Committee (Mar. 26, 2014)

Agenda

A. Overview
   - Data Breach Basics and Statistics

B. Public Enforcement
   - The FTC
   - State Attorneys General

C. Litigation
   - Consumer Class Actions
   - Credit Union Class Actions
   - Shareholder Derivative Suits

D. Prophylactic Steps
   - Insurance
   - Industry and Regulatory Standards
   - Consumer Agreements

PART A – Data Breach Overview

Data Breach Statistics: Lost and Stolen Records

- According to the Ponemon Institute, the average number of records lost to typical data breach was 23,647 per breach
- Ponemon does not track what it considers “catastrophic” or “mega” breaches—100,000+ compromised records—as such breaches have been infrequent and atypical
- But several “mega” breaches have brought the issue into focus: Most prominently, Target may have lost 70 million customer records, including as many as 40 million credit card records
- Trend Micro Security predicts one “mega breach” per month going forward

Data Breach Statistics: Cost of Breaches

- Ponemon reports that average cost of typical data breach at $5.4 million per breach ($188/record), including
  - Detection
  - Escalation
  - Notification
  - Remediation
  - Lost business

Data Breach Statistics: Cause and Extent of Breaches

- Malicious or criminal attacks are the most common cause of data breach (37%), followed closely by human error (35%) and system glitch (29%)
- The **Privacy Rights Clearinghouse** (affiliated with plaintiffs' lawyers in California) lists over 600 reported data breaches in 2013 and more than 60 already in 2014

Data Breach Overview: Industries at risk

- Virtually all businesses are at risk
- Observers believe that some industries face heightened risks, including:
  - Healthcare / pharmaceutical
  - Financial services
  - Infrastructure (transportation, communications, energy)
  - Retail, hospitality, and other consumer-facing businesses
  - Technology
  - Education

Data Breach Overview: New Developments

- The stakes of data breach were already high when news broke last week of the “Heartbleed” bug.
- Heartbleed undermines encryption technology (Open Secure Socket Layer or OpenSSL) used by nearly two-thirds of all websites to secure transmissions from browsers
- Many companies have announced that they were affected by Heartbleed; will disclosure of “mega breaches” follow?
- Plaintiffs may argue that bugs like Heartbleed undermine a primary defense to most state notification statutes
- Many statutes provide safe harbor if compromised records were encrypted and that encryption remains secure

PART B – Enforcement

Enforcement: Overview

- In the absence of comprehensive federal legislation, other enforcers are stepping in to regulate by adjudication/litigation, most notably:
  - the FTC
  - State Attorneys General

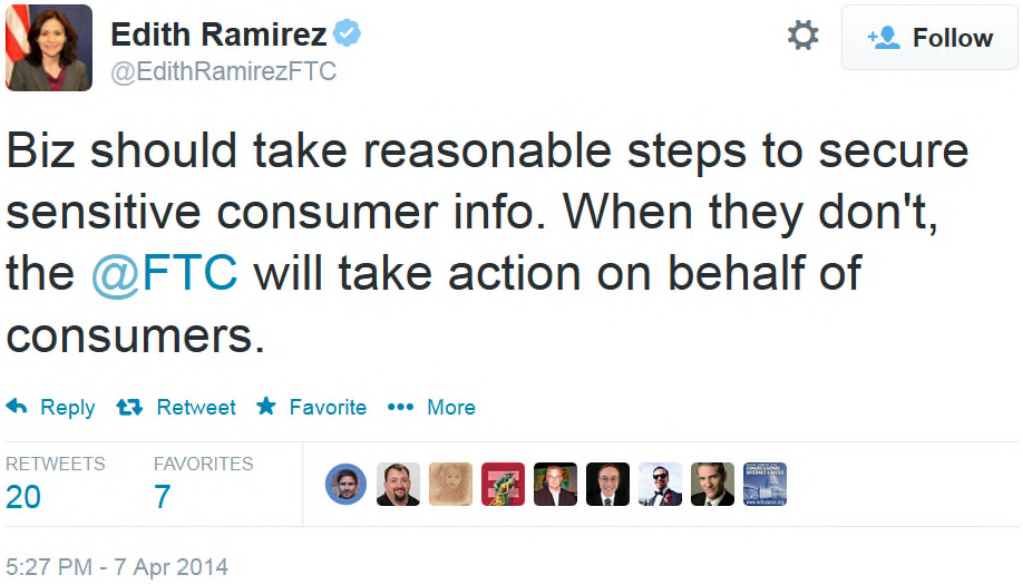
FTC Enforcement: Authority & Approach

- Section 5 of the FTC Act "empowers and directs" the FTC "to prevent persons … from using unfair or deceptive acts or practices in or affecting commerce" 15 U.S.C. § 45(a)
- The FTC has eschewed promulgating any regulations, instead applying a "reasonableness" standard on a case-by-case, fact-specific basis
- On April 7, a federal court approved the FTC's approach, holding that the FTC can bring data breach actions under the "unfair" prong, without first issuing standards (*FTC v. Wyndham Worldwide Corp.*, No. 13-1887 (D.N.J.))

FTC Enforcement: Increased Activity

The District Court did not rule on liability and was clear that its "decision does *not* give the FTC a blank check to sustain a lawsuit against every business that has been hacked," but the FTC may think differently

Soon after the decision, the FTC Chair tweeted:



MAYER·BROWN

FTC Enforcement: Recent Consent Decrees

- As of Q1 2014, the FTC had brought and settled 50 data breach actions
- The FTC's case-by-case approach (as opposed to regulation) makes it difficult to determine what will trigger agency action, but trends are emerging
- In 2013, the FTC settled four enforcement actions:

CBR Systems	Compete Inc.	TRENDnet	Accretive Health
Credit Card Hack	Unsecured Credit Card Info Sent Over the Internet	Security System Hack	Laptop Theft

FTC Enforcement: Common Consent Decrees

Consent decrees entered in 2013 contained the following common features—companies agreed to:

1. Designate dedicated data-security personnel
2. Identify "material internal and external risks"
3. Implement "reasonable safeguards" to control risks
4. Develop "reasonable steps" to select secure vendors
5. Evaluate, monitor & adjust regularly over 20-year period

FTC Enforcement: Case to Watch

- In addition to Wyndham, one other company, LabMD, has refused to settle with the FTC
- Previous attempts by LabMD to contest the FTC's authority faltered in the Eleventh Circuit (petition dismissed for lack of jurisdiction) and a D.C. District Court (complaint voluntarily dismissed)
- LabMD has since filed suit in N.D. Georgia to enjoin the FTC proceedings, and the FTC moved to dismiss, citing *Wyndham*

State AG Enforcement: Investigation

- Many states have data-breach notification laws
- AG investigations and task forces are nothing new, but several AGs have ramped up efforts in light of recent breaches
- For example, the Connecticut and Illinois AGs recently launched probes after hackers bought and sold up to 200 million social security numbers pilfered from an Experian-owned database
- Other AGs, such as Vermont's William Sorrell, have begun holding roundtables to discuss potential legislation
- And AGs have begun coordinating on privacy issues, as with a 18-state, $7 million settlement regarding Google's street view vehicles

State AG Enforcement: Actions

- Several AGs have moved beyond investigation to enforcement
- For example, California AG Kamala Harris filed and quickly settled an action in early 2013 alleging that Kaiser Permanente violated state unfair competition and breach notification laws by waiting too long (four months) to disclose a 2011 breach
- Kaiser agreed to pay $150,000 to improve security protocols, and to provide notice of future breaches on a rolling basis rather than after investigation concludes
- Indiana AG Greg Zoeller reached a similar accord with health insurer WellPoint in 2011 ($100,000 settlement)

State AG Enforcement: Guidance

- In 2013, California AG Harris issued a report discussing impact of data breaches on consumers
- In February 2014, Harris issued *Cybersecurity in the Golden State*, a guidance for smaller businesses that lack resources for full-time security personnel
- Enforcement action may not be far behind: After issuing a guidance document for mobile device security (*Privacy on the Go*) in January 2013, Harris brought suit against Delta Airlines for violation of California's Online Privacy Protection Act (later dismissed)
- Companies should pay close attention to AG reports/guidance

Other Entities

- **DOJ**—which discovered the Target hack—has launched its own investigations (so far, enforcement efforts have focused mostly on criminal prosecution of hackers and thieves)
- **Congress** has called representatives of Target and Neiman Marcus to testify at committee hearings, requesting documents in the process
  - Congressional investigations and reports
- The **SEC** issued a guidance in 2011 regarding cybersecurity disclosures
- Companies operating abroad should be aware that the **EU** and **APEC** are also considering additional cybersecurity rules

PART C – Litigation

Data Breach Litigation: Overview

- Data breach class actions are nothing new. But the scope and number are unprecedented: More cases are being filed in the aftermath of recent, high-profile breaches (over 70 alone versus Target)
- In the past, courts have been skeptical of data-breach claims, and a body of case law exists to support defendants
- The question is whether courts begin to relax requirements on data breach plaintiffs as public perception increases and intensifies
- So far, the answer is mostly 'no'

Data Breach Litigation: Consumer Class Actions

- Customers have launched hundreds of class actions against Target, Neiman Marcus, Michaels, BCBS and others in the past five months (*e.g.*, *Kirk v. Target Corp.*, No. 13-cv-5885 (N.D. Cal.))
- Plaintiffs typically allege that businesses failed to adequately safeguard consumer info and gave insufficient and untimely notice of breach
- Typical cases assert causes of action for negligence, common-law invasion of privacy, and violation of state notification, unfair competition, and consumer protection laws

Data Breach Litigation: Credit Union/Bank Class Actions

- In addition to customers, banks and credit unions have started bringing class actions against Target and others (*e.g.*, *Umpqua Bank v. Target Corp.*, No. 14-cv-00643 (D. Minn.)).
- The complaints assert the same theories as the consumer class actions, but seek damages for administrative expense, lost interest, transaction fees, and lost customers
  - More likely to satisfy standing requirements
- The Consumer Bankers Association claims its members have reissued over 15 million debit/credit cards at a cost of $153 million in response to the Target breach alone

Data Breach Litigation: Shareholder Derivative Suits

- Shareholders have also brought derivative suits against companies victimized by data breach (*e.g.*, *Collier v. Steinhafel*, No. 14-cv-00266 (D. Minn.))
- The suits allege breach of fiduciary duty, abuse of control, gross mismanagement, and waste of resources against corporate officers and directors
- Specifically, the suits charge that board members and executives knew or should have known that a company failed to meet industry standards, leaving customer info vulnerable to attack

Data Breach Litigation: Attacking Individual Claims

- Under Article III of the Constitution, plaintiffs must suffer concrete injury-in-fact to sue in federal court
- In *Clapper v. Amnesty Int'l USA*, the Supreme Court held that plaintiffs who feared their communications would be subject to surveillance lacked standing to sue—and that it was not enough to alleged that they incurred costs to avoid the risk of surveillance (such as cross-country flights for in-person meets)
- The Court held that a "theory of *future* injury is too speculative to satisfy" Article III
- Defendants have argued that this standing requirement should be applied in privacy cases; plaintiffs have tried to limit the decision's reach to the NSA context.

Data Breach Litigation: Attacking Individual Claims

- Before *Clapper*, courts disagreed whether increased risk of identity theft alone was enough to satisfy Article III. *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (no standing)
- Since *Clapper*, several courts have dismissed data breach suits where plaintiffs couldn't allege actual misuse of data or identity theft

- *Galaria v. Nationwide Mutual* (S.D. Ohio 2014, No. 2:13-cv-118) (network hack)
- *In re Barnes & Noble* (N.D. Ill. 2013, No. 1:12-cv-08617) (pin pad hack)

- *Polanco v. Omnicell* (D.N.J. 2013, No.1:13-cv-01417) (laptop theft)
- *In re LinkedIn User Privacy Litig.* (N.D. Cal. 2013, No. 5:12-cv-03088) (network hack)

Data Breach Litigation: Attacking Individual Claims

However, two recent decisions have allowed data breach claims to go forward, albeit in limited form:

In re Sony Gaming (S.D. Cal. 2014): Court dismissed 43 of plaintiffs' 51 claims under the laws of 9 states for lack of standing, but allowed 8 claims under consumer protection laws of California, Florida, Michigan, and New Hampshire. But the surviving claims were limited to injunctive relief and restitution (*i.e.*, the purchase price of a PlayStation gaming console), rather than actual damages, which plaintiffs could not allege. For injunctive/restitutionary relief statutes, a "credible threat" of harm was enough

In re LinkedIn Data Privacy Litig.(N.D. Cal. 2014): After dismissing plaintiff's complaint for lack of Article III standing, the court allowed an amended complaint for false advertising on the theory that plaintiff would not have purchased LinkedIn's premium service but for a statement in the Privacy Policy that information would "be protected with industry standard protocols and technology." Reliance on the alleged promise was enough for standing.

Data Breach Litigation: Attacking Class Claims

- Of course, some plaintiffs may be able to allege that their personal information was accessed and misused
- Defense argument: Differences between class members who did and did not suffer injury should predominate over common issues, preventing class certification
- Under *Comcast Corp. v. Behrend*, plaintiffs would have the burden of proving that there is a workable model for assessing damages on a classwide basis
- But some lower courts have been resistant to *Comcast* and have given it a narrow reading

Data Breach Litigation: Settling Class Claims

- If a business must settle a data breach class action, it will want to secure finality and certainty to the greatest extent possible
- Consider crafting broad class definitions (and accompanying releases) that do encompass users who cannot identify specific actual damages
- A federal court in Florida recently finally approved just such a settlement in a data breach class action stemming from looted laptops (see *Curry v. AvMed, Inc.*, S.D. Fla. No. 1:10-cv-24513)
- AvMed paid $3 million to settle claims arising from a pre-2009 purchase of AvMed products ($10-$30 per customer)

Data Breach Litigation: Settling Class Claims

- TJ Maxx settlement in 2008 of data breach class action provides another point of comparison
- The TJ Maxx breach involved 45 million credit cards (similar to the number reported in connection with Target)
- TJ Maxx settled 25 consolidated class actions as follows:
  - Up to $1 million to customers w/o receipts
  - Up to $10 million to customers w/ receipts ($30/claimant)
  - $6.5 million in plaintiffs' attorneys fees
  - 3 free years of credit monitoring said to cost $177 million

Data Breach Litigation: Statutory Damages

- Congress or States could pass laws (or amend existing laws) providing a private right of action or statutory damages
- Traditionally, such rights/damages have not eliminated the requirement that plaintiffs prove injury in fact
- But a recent 9th Circuit decision (not alleging data breach) held that plaintiffs need not allege actual injury to sue for willful violation of the FCRA (*Robbins v. Spokeo, Inc.*, No. 11-56843)
- On the other hand, the California Court of Appeal held a plaintiff alleging data breach must suffer actual damage to state a claim for statutory damages under California's Medical Information Act, which has a private right of action (*Univ. of Cal. v. Super. Ct.*, 220 Cal. App. 4th 549)

PART D – Prophylactic Steps

An ounce of prevention …

- The best way to prevent against data breach lawsuits is to prevent data breaches in the first place
- But no security is foolproof; breaches will occur
- How can businesses defend against or minimize the effects of lawsuits in the event of breach?
  - Adopt and follow reasonable procedures to guard against breaches
  - Obtain cybersecurity insurance where available
  - Revise customer agreements to secure contractual protections for defendants where feasible

Internal Security Compliance

- It may seem obvious, but one of most important things a company can do to prepare for breach lawsuits is to follow its own internal procedures
- Senator Rockefeller's report on the Target hack chastised Target for failing to heed automated warnings from its anti-intrusion software
- Plaintiffs are bringing lawsuits that focus on a business's failure to respond earlier to signs of intrusion (see *Mancias v. Target Corp.*, No. 3:14-cv-00212 (N.D. Cal.))

Sources for Security Standards

- As FTC Chairwoman Ramirez said, not every breach will be a violation of law. Liability may well turn on whether the business has adopted and followed reasonable procedures
- Companies should consider their policies in light of evolving cybersecurity standards:
  - As outlined above, FTC Consent Decrees outline breach prevention protocols that the FTC might find acceptable
  - State AG guidance documents provide additional suggestions for breach prevention
  - AG enforcement actions reveal how quickly states expect companies to notify consumers of breach

Sources for Security Standards

- Industry groups such as the Retail Industry Leaders Association (RILA) have launched initiatives designed to improve cyber-security and lobby legislators
- The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity makes what it calls “informative references”
- NIST is clear that its references should not become liability standards, and no framework should be seen as “one-size-fits-all”
- But even considering (and adopting other) accepted standards can help demonstrate that company was not negligent

Cybersecurity Insurance

- Application of CGL policies to data breach tends to turn on whether customer information was "published"
- A recent decision suggests that publication of purloined data may trigger standard CGL policies (see *Recall Total Info. Mgmt. Inc. v. Fed. Ins. Co.*, No AC 34716 (Conn. Ct. App.) (finding no publication and thus no coverage)
- But another recent case suggests CGL policies don't apply unless the insured did the "publishing" (see *Zurich Am. Ins. v. Sony Corp.*, No. 651982 (NY Sup. Ct.))
- Companies should consult their existing policies and counsel to see whether data-breach coverage might exist and otherwise consider purchasing additional cyber-insurance

Customer Agreement Changes

- Courts have yet to address these issues, but appropriate disclosures in customer agreements may help minimize data breach liability, for example:
  - Enhanced disclosures regarding collection and use of data
  - Enhanced disclaimers and limitations on liability
- And enforceable arbitration agreements that contain class-action waivers can minimize the risk of all class actions, not just data-breach litigation

MAYER·BROWN