McDermott Will & Emery

U.S. Privacy and Data Protection: 2013 Year in Review and a Look Ahead to 2014

January 28, 2014

www.mwe.com

Agenda & Speakers

McDermott Will & Emery

- **Tony Bongiorno** – Litigation Highlights
- **Ed Zacharias** – U.S. Healthcare Law
- **Heather Egan Sussman**, CIPP/US – Key State Law Developments
- **Ann Killilea** – U.S. Safe Harbor Developments
- **Dave Gacioch** – Enforcement Actions and Settlements
- **Julia Jacobson** – Look Ahead to 2014

McDermott Will & Emery

Litigation Highlights

Anthony A. Bongiorno
617.535.4044
Email: abongiorno@mwe.com

Litigation Highlights – Overview

McDermott Will & Emery

OVERVIEW

- High Profile Data Breaches at Major Retailers
- *Genesco v. Visa* Litigation
- Telephone Consumer Protection Act

High Profile Data Breach at Major Retailer

McDermott Will & Emery

- Hackers penetrated that retailer's computer systems and gained access to a large number of:
  - Credit card numbers;
  - Encrypted PINs;
  - Names;
  - Email addresses;
  - Mailing addresses.
- Millions of customers affected
- Black-market websites selling credit card numbers were inundated with new listings from the breach

Resulting Litigation: Claims

McDermott Will & Emery

- Plaintiffs' lawyers race to the courthouse
  - First suit filed in Florida within 48 hours of the announcement
  - At least 70 suits as of January 15, 2014, most putative class actions
- Allegations include:
  - Negligence: failure to safeguard the data
  - Invasion of privacy: failing to safeguard customer information
  - State-law claims, including implied covenants and unfair trade practices

Resulting Litigation: Damages Sought

McDermott Will & Emery

- Consumer class action suits seek:
  - Actual damages (the challenge)
  - Restitution
  - Statutory penalties
  - Punitive damages
  - Injunctive relief
  - Attorneys' fees

The Plaintiffs' Hurdle: Standing?

McDermott Will & Emery

- Absent allegations of actual identity theft, plaintiffs face a high standing hurdle
- *Clapper v. Amnesty International, USA* (S.Ct. 2013)
  - Court rejected Amnesty's challenged to Foreign Intelligence Surveillance Act for failure to satisfy Article III standing requirement
    - **Threat** of Gov't eavesdropping on plaintiffs' calls with foreigners **was not a sufficient "injury"** to confer standing

Clapper: The Standard

McDermott Will & Emery

- To confer standing, a threatened injury must be "certainly impending"
  - Future chance that the Government *might* intercept plaintiff's calls not sufficient
- Plaintiffs cannot "manufacture standing" by inflicting harm on themselves based on fear of non-imminent future harm
  - Costs incurred in avoiding government eavesdropping not sufficient either

Clapper's Effect on Litigation to Date

McDermott Will & Emery

- Data breach ≠ "certainly impending" injury
- The courts have already applied *Clapper* to dismiss data breach and data security cases
  - *In re Barnes & Noble PIN Pad Litigation* (N.D. Ill. Sept. 2013)
    - Increased risk of identity theft not "certainly impending" harm
    - Costs incurred to minimize risk of identity theft not an injury under Art. III
  - *Hammer v. Sam's East, Inc.* (D. Kan. July 16, 2013)
    - Increased risk of identity theft did not confer standing
  - *Polanco v. Omnicell, Inc.*, (D.N.J. Dec. 26, 2013)
    - Costs incurred to reduce risk following data breach did not confer standing

Clapper: "Not So Fast"

McDermott Will & Emery

- Not all courts agree that *Clapper* bars data breach suits absent identity theft
  - *In re Sony Gaming Networks and Customer Data Security Breach Litigation*
    - "*Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be 'real and immediate.'"
    - "The Court finds that Plaintiff's allegations that the Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion sufficient to establish Article III standing at this stage in the proceedings."

Further Litigation From High Profile Data Breaches

McDermott Will & Emery

- Existing suits by banks that incurred losses in reissuing cards and paying fraudulent charges may survive motion to dismiss stage
- Banks have alleged:
  - Negligence in failing to safeguard the data
  - Breach of Contract/negligent misrepresentation regarding compliance with credit card company regulations
  - State law unfair practice and deceptive practice claims for failure to safeguard the data

Future Litigation Risks??

McDermott Will & Emery

- A possible second wave of suits by identity theft victims may be viable under *Clapper*
  - Phishing: “Hello. You have been affected by the recent [Company] data breach. As a result your credit card and bank account have been compromised. [Company] is providing a free data monitoring service. In order to proceed and issue a new credit card number, may I please confirm your name and social security number?”
  - Spearphishing: “Hello Mr. Bongiorno. I see that you shopped at [Company] on November 29, 2014. May I please verify your social security number?”

Takeaways

McDermott Will & Emery

- More data breaches – and more litigation – expected
- *Clapper* provides a good "first wall defense" against many consumer suits
- Retailers still face litigation by banks and likely cases by victims of actual identity theft

Genesco v. Visa

Genesco v. Visa

McDermott Will & Emery

- Background
  - Genesco is a retailer with over 2,400 stores.
  - In 2009-2010, Genesco experienced an attack by hackers targeting credit and debit card data from Genesco's computer network.
  - Hackers installed malware into Genesco's computer system to capture credit and debit card data as it was being transmitted from Genesco's system to acquiring banks for transaction approval.

Relationship Between Payment Brand, Retailers, and Banks

McDermott Will & Emery

Payment brand (e.g., Visa)
Banks enter into agreements with Visa to be an "acquiring bank" and/or an "issuing bank."

When a customer pays for a purchase at a retailer with a payment brand card, the **acquiring bank** collects the purchase amount from the **payment brand** and pays the **retailer**.

The **payment brand** collects the purchase amount from the **issuing bank.** The **issuing bank** collects the amount of the transaction from the individual cardholder who made the purchase

Retailer

Consumer

Visa Contracts With Banks

McDermott Will & Emery

- Visa's contracts with issuing and acquiring banks are governed by the Visa International Operating Regulations ("VIOR").
- The VIOR incorporate industry-wide standards for data security: the Payment Card Industry Data Security Standards ("PCI-DSS"). The PCI-DSS are designed to protect payment card account information.
- A data breach *may* mean a retailer failed to follow the PCI-DSS – but could also be the result of sophisticated hackers accessing data, even when the retailer followed the PCI-DSS.

Genesco – Fines Assessed by Visa

McDermott Will & Emery

- After Genesco's data breach, Visa assessed 3 types of fines against the acquiring banks pursuant to the Operating Regulations:
  - Fines for Genesco's PCI-DSS alleged noncompliance (minimal $$)
  - Fines for alleged operating expense recovery
  - Fines for alleged counterfeit fraud recovery
- Fines totaled **$13,298,900.16.** The bulk of the fines were for operating expense and counterfeit fraud recovery.
- Under its agreements with the acquiring banks, Genesco reimbursed the acquiring banks for the fines.

Genesco's Lawsuit

McDermott Will & Emery

- Genesco sued Visa in March 2013 seeking to recover the $13+ million in fines that Visa assessed.
- In its Complaint, Genesco alleges:
  - Visa breached its contracts, because it did not have a factual basis to assess fines under the VIOR:
    - Genesco claims that not all Visa cardholder accounts were impacted by the data breach.
    - Genesco also claims that it was not in violation of the PCI-DSS when the data breach occurred.
  - Visa's business practices in assessing fines against the acquiring banks violates the California Unfair Business Practices Act.
  - The fines that Visa assessed are unenforceable penalties.

Status of *Genesco* Litigation

McDermott Will & Emery

- Visa filed a Motion to Dismiss Genesco's unjust enrichment and California Unfair Competition Law (UCL) claims.
- The court denied Visa's motion in July 2013.
- Genesco filed a motion for partial summary judgment, asserting that the PCI-DSS fines were unenforceable penalties.
- The court denied the motion in November 2013, but left the door open for a renewed motion at a later date after additional discovery.
- Discovery is ongoing in this case.

Takeaways from *Genesco* Litigation

McDermott Will & Emery

- Takeaways
  - Currently, payment card companies can unilaterally assess fines under contracts with their banks.
  - Retailers indemnify acquiring banks.
    - Thus, acquiring banks have little incentive to change the system.
  - *Genesco* is the first case in which a retailer has challenged the authority and practices of one of the payment card companies.
  - *Genesco* litigation could lead to changes in the relationship between payment card companies, retailers and acquiring banks following a data breach, essentially flipping the leverage.

Takeaways from *Genesco* Litigation

McDermott Will & Emery

- Recent high profile data breaches have put the issue of credit/debit card transactions in the spotlight.
- Issuing banks may be the next group to litigate over data breaches.
  - Issuing banks have started to sue retailers in putative class actions following data breaches.
- Will payment card companies and/or acquiring banks also be sued by issuing banks for failure to keep consumer data safe.

Telephone Consumer Protection Act

New Rules & Expanded Liability

Telephone Consumer Protection Act: Overview

McDermott Will & Emery

- The Telephone Consumer Protection Act of 1991 ("***TCPA***") regulates calls made by automated dialing systems or using an artificial or prerecorded voice.
- The TCPA imposes limits on:
  - Calls to residential landlines
  - Calls to mobile phones
  - Text messages and unsolicited faxes

Telephone Consumer Protection Act: Penalties

McDermott Will & Emery

- The TCPA imposes significant financial penalties:
  - $500 per call made in violation of the law, increased to $1,500 for willful violations
  - Government agencies and private plaintiffs can enforce the TCPA and actions can be brought in state court
- “Calls” include text messages and similar communications.

Telephone Consumer Protection Act: New Rules

McDermott Will & Emery

- The TCPA delegates significant rulemaking authority to the FCC. The FCC promulgated new rules in February 2012.
- New Rule effective October 2013: "Express prior written consent" is required for:
  - telemarketing calls to a wireless telephone number when an artificial or prerecorded message or automatic telephone dialer system (ATDS) is used;
  - telemarketing text messages sent using an ATDS; or
  - telemarketing calls to a residential landline telephone number using an artificial or prerecorded message.

Telephone Consumer Protection Act: New Rules, *cont.*

McDermott Will & Emery

- Express Prior Written Consent
  - written agreement signed by the person called that clearly authorizes delivery of advertising or telemarketing messages using an ATDS or an artificial or prerecorded voice message
  - written agreement may be "signed" electronically using any method recognized under the federal E-SIGN Act
- Consent cannot be a required condition for a purchase or transaction.
- Caller bears the burden of proving called party's consent.

  - .

Telephone Consumer Protection Act: New Rules, *cont.*

McDermott Will & Emery

- New Rule: Artificial or prerecorded telemarketing messages must include an automated, interactive mechanism that enables the called person to opt out of receiving future prerecorded messages (effective January 14, 2013).
- New Rule: Telemarketers must ensure that no more than three percent (3%) of calls answered by a person are "abandoned" (i.e., not answered by the telemarketer within two (2) seconds after the called person answers) during a thirty-day calling campaign period (effective November 16, 2012).

Telephone Consumer Protection Act: Exceptions

McDermott Will & Emery

- Debt collection calls
  - Unless they contain advertising.
- Calls to residential lines by HIPAA-regulated entities.
- “Informational” calls: flight status, appointment reminders.
  - “Written” consent is not required for such calls.
  - Cannot have any promotional content.

Telephone Consumer Protection Act: Key Developments 2013

McDermott Will & Emery

- DISH Network's Challenge to FCC Guidance
  - DISH sought guidance from FCC regarding liability for violations by third-party call centers contracted by companies.
  - FCC Guidance: expansive definition of agency.
  - DISH did not like the FCC's answer, so it brought a legal challenge.
  - FCC now admits its guidance on third-party liability is not binding – but the guidance shows the position the FCC is likely to take in TCPA enforcement proceedings.

Telephone Consumer Protection Act: Key Developments 2013, *cont.*

McDermott Will & Emery

- Uesco's Supreme Court Cert Petition
  - Another challenge to a company's liability for violations by its vendors that sent faxes on the defendant's behalf.
  - The Court found the defendant not liable for much of the vendor's conduct.
  - Plaintiff now seeking review, arguing the expansive agency doctrine.
  - If the Supreme Court takes the case, it may settle the law in this area.

Telephone Consumer Protection Act: Key Developments 2013, *cont.*

McDermott Will & Emery

- J.C. Penney Fails to Defeat Class Action
  - J.C. Penney faces a putative class action for text messages allegedly sent in violation of the TCPA.
  - Court: J.C. Penney's offer of judgment did not moot action based on unsolicited texting; the case continues.
- Standard Mutual Insurance Co. v. Lay
  - There is a split in authority whether TCPA damages are punitive damages that cannot be paid by insurance (as a matter of public policy).
  - Illinois Supreme Court: TCPA damages are remedial, not punitive, and are therefore insurable.

What Should Businesses Consider?

McDermott Will & Emery

- Review current calling practices.
  - The new rules are complex. Review your existing policies –and the new regulations under the TCPA.
  - Audit current practices to make sure your employees / vendors are complying with your policies.
- Update the way in which you secure consent from customers, as needed.
  - Written consent agreements should be drafted in broad terms.

What Should Businesses Consider?

McDermott Will & Emery

- Keep good records of consent and calling practices.
  - The burden is on businesses to prove consent in TCPA cases.
- When hiring vendors to run calling operations:
  - Review agreements to ensure that they explicitly require TCPA compliance and consider reps and warranties.

What Should Businesses Consider?

McDermott Will & Emery

- Review whether your business liability policy insures TCPA damages.
  - The trend seems to be to permit such insurance coverage.
- Consider a consumer arbitration clause that encompasses TCPA claims.
  - *Cyganiewicz v. Sallie Mae* (D. Mass. Oct. 24, 2013)
    - Court dismissed consumer case in favor of arbitration based on broad consumer arbitration agreement.

McDermott Will & Emery

HIPAA & U.S. Healthcare Law

Edward G. Zacharias
617.535.4018
Email: ezacharias@mwe.com

Final HIPAA Omnibus Regulations

McDermott Will & Emery

- Key Topics
  - Business Associates (BAs) and their Subcontractors
  - Vicarious Liability for BAs and Subcontractors
  - Revised Definition of Breach
  - Use and Disclosure of PHI for Marketing
  - Restrictions on Sale of PHI
  - Enforcement

HIPAA Guidance

McDermott Will & Emery

- OCR Guidance since publication of final regulations
  - Refill reminders exception to prohibition on use of PHI for marketing
  - Model notice of privacy practices
  - Model business associate agreement
  - Use and disclosures of PHI of deceased individuals
- Future guidance?
  - Types of entities that do and do not fall within definition of BA
  - Minimum necessary
  - Breach risk assessments for frequently occurring scenarios
  - Updates to encryption guidance
  - HITECH Act accounting of disclosures rule making

2013 OCR Enforcement Activity

McDermott Will & Emery

- Hospice of North Idaho
  - $500K and CAP (2 yrs)
- Idaho State University
  - $400K and CAP (2 yrs)
- Shasta Regional Medical Center
  - $275K and CAP (1yr)
- WellPoint, Inc.
  - $1.7 million (no CAP)

2013 OCR Enforcement Activity, cont.

McDermott Will & Emery

- Affinity Health Plan, Inc.
  - $1,215,780 and CAP (120 days)
- Adult & Pediatric Dermatology, P.C.
  - $150,000 and CAP (until date OCR approves implementation of CAP)
- 2014 Enforcement Predictions
  - Increase in reported breaches under new standard
  - Sustained or Increased OCR Enforcement Activity
    - November OIG Report re: OCR Enforcement of HIPAA Security Rule
  - State Attorneys General Enforcement Activity

McDermott Will & Emery

Key U.S. State Law Developments

Heather Egan Sussman
617.535.4177
Email: hsussman@mwe.com

Key U.S. State Law Developments

McDermott Will & Emery

- Breach Notification Laws
  - VT: 14 day notice, now covers financial institutions
  - ND: adds medical and health information to definition of PII
  - CA: adds online account log-in credentials to definition of PII requiring notification in the event of a breach
- Employer's Access to Social Media Accounts
  - Password protection legislation is pending or has been introduced in more than 30 states
  - 8 states passed such laws in 2013, including AK, CO, NV, NJ, NM, OR, UT and WA

Key U.S. State Law Developments

McDermott Will & Emery

California Online Privacy Protection Act (CalOPPA)

- California Business And Professions Code Section 22575 – 22579
  - Amendments to Section 22575 signed into law on Sept. 27, 2013
  - Amendments to Section 22575 effective as of January 1, 2014
- Under amended Section 22575, website owners/operators MUST:
  (1) Disclose how they respond to Do Not Track, AND
  (2) Disclose whether third parties are collecting data for IBA purposes on or through the website or service
  - Operator can satisfy requirement under (1), above, by complying with DAA's Self-Regulatory framework for OBA (so called "safe harbor")

McDermott Will & Emery

High-Stakes International Drama: ***Safe Harbor Alive and Well***

Ann Killilea
617.535.3933
Email: akillilea@mwe.com

The Program Bill

McDermott Will & Emery

- Setting The Stage: Brief Safe Harbor Overview
- The Performance: Heated Dialogue and Action
- Backstage: Behind The Scenes – The Real Work
- Sequel: Predictions for 2014
- Red Carpet Reviews

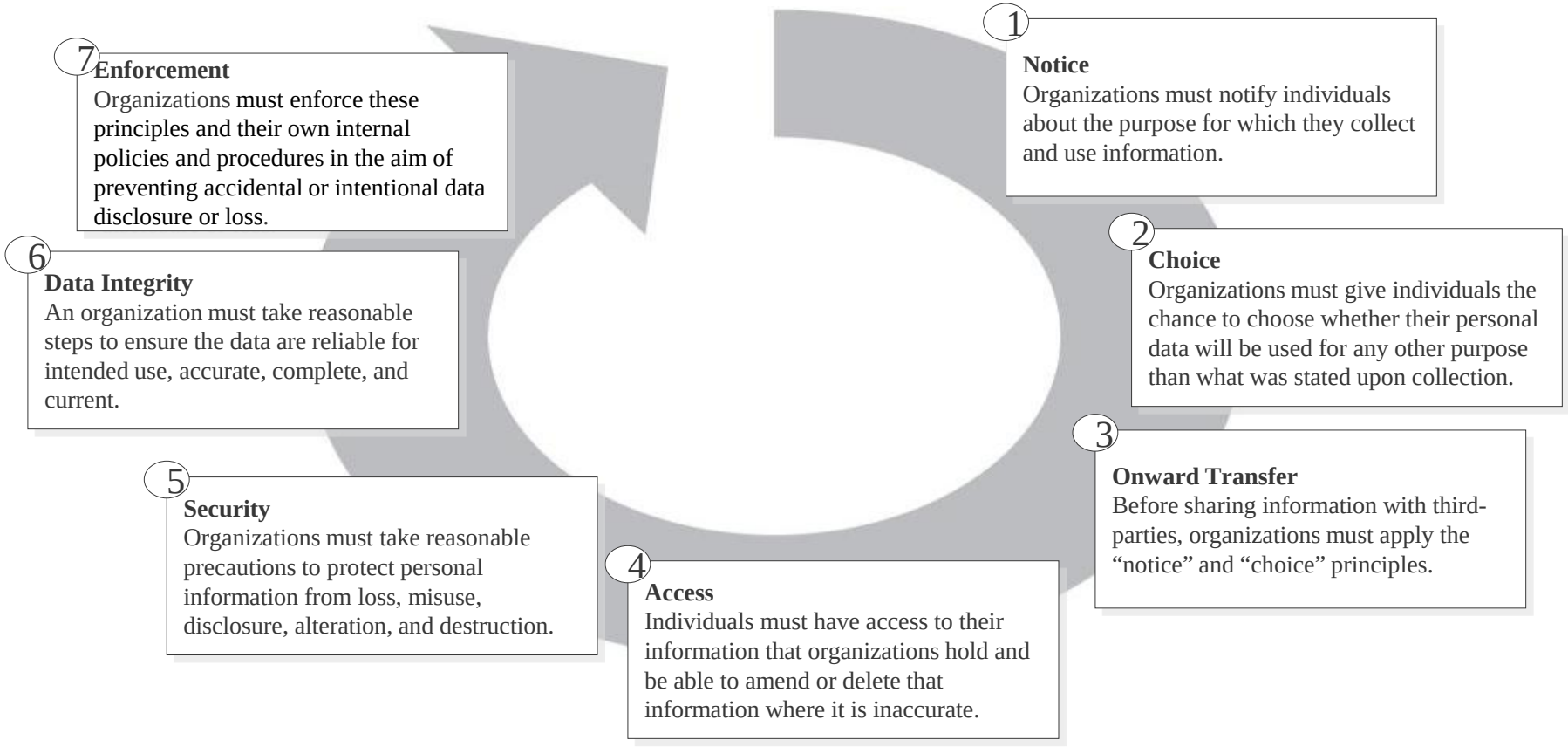
Setting the Stage: Brief Safe Harbor Overview

McDermott Will & Emery

- Adequacy Requirement.
- Under Safe Harbor, U.S. company becomes adequate unto itself; applies EU-like data protection to EU data subjects.
- Goals : (1) To allow free flow of regulated personal data from EU Member States and the U.S.; and (2) To protect data according to Safe Harbor Principles.
- Voluntary, But Binding, Commitments.
- Transparency of company privacy policies.
- Incorporation of Safe Harbor Principles in company privacy policies and practices/enforcement mechanisms.

Safe Harbor Privacy Principles -- Seven

McDermott Will & Emery



The Performance: Heated Dialogue (E.U.)

McDermott Will & Emery

- Surveillance accusations.
- VP, European Commission (Viviane Reding): "…a loophole" that may not be so safe after all."
- European Parliament Member (Jan Philipp Albreacht): wants a review and an express reauthorization of Safe Harbor; otherwise discontinue.
- Chairman of Article 29 Working Party: reminder that member states can suspend data flow where a "substantial likelihood" exists that Safe Harbor is violated.
- EC Report (Nov. 2013): critical, recommended 13 improvements but not suspension.

The Performance: Action (U.S.)

McDermott Will & Emery

- As of Dec. 2013, 4,327 companies have certified since 2000.
- 3328 companies are now listed as current.
- Industries represented – management consulting, cloud providers, advertising and information services/data processing companies.
- Often, a preferred compliance mechanism for U.S. multinational companies.

Backstage: Behind the Scenes – The Real Work

McDermott Will & Emery

- Form cross-functional privacy and data protection team.
- Develop global privacy policy reflecting Safe Harbor principles.
- Ensure training on, and availability of, policy.
- Provide independent recourse for complaints.
- Establish accountable/identifiable privacy contact resource.
- Attest on DOC website that company is properly certified–public process.
- Submit to FTC enforcement if company fails to comply.
- Renew annually and reassess compliance prior to renewal.

Result: A corporate-wide privacy and data protection program compliant with Safe Harbor principles and EU data protection requirements.

The Director's Chair: FTC Enforcement (Scene 1)

McDermott Will & Emery

- Subject to government enforcement of federal and state unfair and deceptive statutes.
- FTC active enforcer of Safe Harbor.
- 10 actions for Safe Harbor violations (2009-2012):
  - Alleged companies deceived consumers by representing certification when in fact certifications has lapsed (6) (2009);
  - Alleged company misrepresented on website that it was Safe Harbor-certified (1) (2009);
  - Alleged specific violations (i.e., notice and choice violations) (3) (2011-2012).

The Director's Chair: FTC Enforcement (Scene 2)

McDermott Will & Emery

- 12 actions for Safe Harbor violations (January 21, 2014):
  - Alleged that companies misrepresented that they held current certifications though certifications had lapsed;
  - Proposed no-fault consent agreements (subject to public comment and final consent orders).
- Cross-section of industries – retail, professional sports, lab science, data broker, debt collection, information security.
- "Enforcement of the U.S.-EU Safe Harbor Framework is a Commission priority," Edith Ramirez, Chairwoman, FTC.

Sequel: Predictions for 2014

McDermott Will & Emery

- Remains a viable and effective compliance mechanism.
- Subject to “tweaking” in response to EU suggestions.
- More FTC enforcement actions to underscore Program’s effectiveness.
- Companies to continue certification/recertification activities.
- In the process, companies build corporate-wide data protection programs.

Program Notes: Resources

McDermott Will & Emery

- Safe Harbor Workbook, EXPORT, GOV, http://export.gov/safeharbor/eg_main_018238.asp.
- Safe Harbor List, EXPORT.GOV, https://safeharbor.export.gov/list.aspx
- U.S,-EU Safe Harbor Overview, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp

McDermott Will & Emery

Enforcement Actions and Settlements

David Quinn Gacioch
617.535.4478
Email: dgacioch@mwe.com

Trends in Non-FTC Enforcement

McDermott Will & Emery

- Increasing number of breaches reported
- More investigative/enforcement resources dedicated by states
  - To enforce both state laws and HIPAA
- More multi-agency investigations
- Slowly-increasing number and size of settlements
- Continued lack of examples of enforcement agencies commencing litigation when no settlement is reached

2013: Multi-State Settlements

McDermott Will & Emery

- A leading information technology company:
  - In March, settled allegations by ~40 state attorneys general that it had collected data from unsecured wireless networks without authorization -- **$7 million**, plus non-monetary terms
  - In November, settled separate allegations by ~40 state attorneys general concerning tracking cookie practices specific to Apple devices -- **$17 million**, plus non-monetary terms

State-by-State

McDermott Will & Emery

- Most active states appear to be:
  - **California**
    - Dedicated, 6-lawyer privacy enforcement unit in AG's office launched in 2012
  - **Connecticut**
  - **Maryland**
    - Dedicated internet privacy enforcement unit launched in 2013
  - **Massachusetts**
  - **New Jersey**
    - Four separate settlements announced in 2013 (not counting multi-state)
  - **Vermont**

2013: Medical Billing Company and Four Pathology Practices

McDermott Will & Emery

- January settlement with Massachusetts AG concerning 2010 improper disposal of pathology medical records of 67,000 patients in unsecured transfer station
  - Resolved both state law and HIPAA-based claims
  - **$140,000** collectively
  - Non-monetary terms

2013: PulsePoint Inc.

McDermott Will & Emery

- July settlement with State of New Jersey concerning display ad coding that allegedly bypassed do-not-track/cookie-related browser settings
  - **$1 million**
  - Non-monetary terms including conspicuous posting of privacy and opt-out practices
  - Five years of independent monitoring

2013: Major US Bank

McDermott Will & Emery

- August settlement with State of Connecticut resolving allegations that bank had not done enough to protect 360,000 customers impacted by 2011 data breach
  - **$55,000**
  - Third-party security audit

2013: Natural Provisions Inc.

McDermott Will & Emery

- September settlement with State of Vermont resolving allegations that store had been slow to notify impacted customers and tighten security in wake of 2012 payment card-related breach
  - **$15,000 civil monetary penalty**
  - **$15,000 in required IT security upgrades**
  - Additional non-monetary terms, including creation and implementation of a WISP

2013: E-Sports Entertainment

McDermott Will & Emery

- November settlement with State of New Jersey for alleged introduction of malware onto 14,000 users' machines to mine for Bitcoins
  - **$1 million payment** (with $675,000 suspended for 10 years)
  - Additional non-monetary terms
  - Independent monitoring

2013: Dataium

McDermott Will & Emery

- November settlement with State of New Jersey resolving allegations of unauthorized “history sniffing” of hundreds of thousands of users’ browsers, and subsequent sale of data
  - **$400,000 payment** (with $301,000 suspended for 5 years)
  - Additional non-monetary terms

2013: Dokogeo

McDermott Will & Emery

- November settlement with State of New Jersey resolving alleged COPPA violation involving collecting of children's information through animated apps
  - **$25,000 payment** (entirely suspended for 10 years)
  - Additional non-monetary terms

2013: Non-Settlement News

McDermott Will & Emery

- **LivingSocial, Inc.**: Joint, public letter from Maryland and Connecticut AGs in May seeking answers in wake of recently-disclosed breach affecting up to 50 million customers
  - Investigation has been out of the news since May
- **Schnucks Inc.**: Missouri AG publicly cleared company of any wrongdoing in wake of recently-disclosed breach affecting 2.4 million customers
  - AG lauded company for cooperating with investigators

2013: Non-Settlement News (Cont'd)

McDermott Will & Emery

- **Delta Airlines**: December 2012 enforcement suit filed by California AG over Fly Delta mobile app dismissed by state court in May
  - California's first such suit under nine-year-old law
  - Dismissed on federal preemption grounds specific to airline industry
  - Court did not address the merits of the underlying privacy claims

Continuing Trend…

McDermott Will & Emery

- Fly Delta case was an outlier: still highly uncommon to see non-FTC enforcement agencies commence litigation without settlement already in place
- High stakes for enforcement authorities to litigate:
  - Risk of negative publicity *AND*
  - Risk of bad precedents

Key Takeaways for Privacy Professionals

McDermott Will & Emery

- Commit the necessary compliance time/resources before a breach occurs
  - Lessens risk that breaches will occur
  - Creates better enforcement positioning if they do occur
- Practice what your company's policies, disclosures, and agreements preach
  - Removes key enforcement agency argument that practice at issue was unfair/deceptive to consumers

Key Takeaways (Cont'd)

McDermott Will & Emery

- When a breach occurs:
  - **Act quickly** to gather basic information and make notifications; do not wait for stated deadlines
  - **Engage enforcement authorities proactively** and cooperatively
  - Keep attorney-client **privilege** issues in mind
  - But **don't hesitate to stand firm** when authorities take unsupported or unreasonable settlement positions

McDermott Will & Emery

FTC Enforcement Actions and Settlements

Heather Egan Sussman
617.535.4177
Email: hsussman@mwe.com

Edward G. Zacharias
617.535.4018
Email: ezacharias@mwe.com

Julia Jacobson
617.535.3881
Email: jjacobson@mwe.com

FTC Settlements

McDermott Will & Emery

FTC Settlements:

- Aaron's Inc. (monitoring technology on rented computers)
- HTC America (software and mobile device vulnerabilities)
- Cbr Systems (unencrypted portable devices) - 20 year consent decree
- Accretive Health (medical billing information on laptop) - 20 year consent decree
- Path, Inc. (app automatically collected contacts data) - $800K penalty and 20 year consent decree – February 2013

FTC Enforcement Action - Internet of Things

McDermott Will & Emery

TRENDNet Inc. Settlement – September 2013

- TRENDNet manufactures Internet–connected home security video cameras called “SecurView”.
- TRENDNet failed to provide reasonable security despite advertising the cameras as “secure”
  - Lived feeds accessible over the Internet without log-in credentials, no encryption for log-in credentials, no response to reports of security problems, etc.
- Failure to provide reasonable security = unfair and deceptive trade practice
- 20 year consent decree that bars inaccurate advertising about security of cameras, implement CISP, third-party security assessments, etc.

Ongoing FTC Enforcement Actions

McDermott Will & Emery

Ongoing 2013 Enforcement Actions

- Wyndham - Security vulnerabilities resulted in fraudulent credit card charges
  - U.S. District Court for the District of New Jersey denied Wyndham's motion to dismiss based on argument that FTC lacks authority to regulate data security (November 12, 2013)
- LabMD Inc. - Information submitted for medical testing related to cancer diagnoses hacked
  - FTC denied motion to dismiss (January 16, 2014): data security is not beyond FTC's reach under FTC Act

McDermott Will & Emery

What's Ahead for 2014

Julia Jacobson
617.535.3881
Email: jjacobson@mwe.com

Heather Egan Sussman
617.535.4177
Email: hsussman@mwe.com

WHAT'S AHEAD IN 2014

McDermott Will & Emery

- Enforcement Activities by California Attorney General under CalOPPA
  - Transparency / Adequacy of Disclosure
- Enforcement Activities by Better Business Bureau's Online Interest-Based Advertising Accountability Program
  - Monitors businesses' advertising practices
  - Enforces the DAA's self-regulatory program, even for companies that are not participating in it

WHAT'S AHEAD IN 2014

McDermott Will & Emery

New Privacy Rights for California Minors Effective January 1, 2015:

- **Cal. BPC §2580 - Minor Marketing Law**: Prohibits *digital advertising and marketing* to California minors of nineteen categories of products and services that are regulated under California law (e.g., alcohol, tobacco products, 'obscene matter,' lethal weapons)

- **Cal. BPC §2581 - Eraser Button Law**: Requires owners of websites, online services and applications and mobile applications directed to or known to be used by California minors to offer a process for California minors to *remove (or have removed) their own posted content and information*. (For more information, see "Right To Erase?" at http://www.e-comlaw.com/e-commerce-law-and-policy/hottopic.asp?id=1394)

WHAT'S AHEAD IN 2014

McDermott Will & Emery

- COPPA Enforcement: January 1, 2014 was the six month anniversary of implementation of final COPPA Rule
  - Focus on Mobile Apps
  - Focus on Social Media
- Internet of Things Enforcement
  - Challenges to FTC's authority to regulate data security under the FTC Act continue to be unsuccessful (LabMD, Wyndham)
  - Proofpoint uncovers "first proven Internet of Things (IoT)-based cyberattack" involving 'smart' appliances: more than 100,000 appliances compromised and used as a platform to launch more than 750,000 malicious email communications (January 16, 2014)

    (See http://www.proofpoint.com/about-us/press-releases/01162014.php.)
  - More data security enforcement actions in store for manufacturers of IoT products

WHAT'S AHEAD IN 2014

McDermott Will & Emery

- Consumer Health Information (CHI) = Information about or related to a consumer's health that is not covered by HIPAA
  - Do consumers expect that CHI will be treated differently than other kinds of personal information?
    - Will other state Attorneys General follow the Illinois Attorney General in questioning privacy practices of health-related digital service providers?
  - LabMD Ruling: Data security for HIPAA-regulated information is not beyond FTC's reach under FTC Act
  - Considerations for 2014: Should CHI receive special treatment?

WHAT'S AHEAD IN 2014

McDermott Will & Emery

Wave of Class Actions will continue in 2014

Consideration for 2014: Add a Class Action Waiver to Dispute Resolution Provisions in B2C agreements

> "YOU AGREE THAT YOU MAY BRING CLAIMS AGAINST THE COMPANY ONLY ON AN INDIVIDUAL BASIS AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE ACTION OR PROCEEDING…"

- Make Class Action Waiver ***Clear and Conspicuous*** in Agreement
- Check Dispute Resolution Provisions of Related Agreements

Wrapping Up

McDermott Will & Emery

- Questions
- Closing Remarks