WINSTON & STRAWN LLP

Defending CCPA's "Reasonable" Safeguards Standard Against an Unreasonable Plaintiff's Bar

September 16, 2019

Today's Webinar Presenters

Sean Wieber
Partner
Chicago
(312) 558-5769
swieber@winston.com

Becky Troutman
Partner
San Francisco
(415) 591-1401
btroutman@winston.com

Alessandra Swanson
Of Counsel
Chicago
(312) 558-7435
aswanson@winston.com

Eric Shinabarger
Associate
Chicago
(312) 558-8823
eshinabarger@winston.com

Roadmap: Where We Are Headed Today

- CCPA's "reasonable" safeguards requirement and how it relates to California's existing breach notification law
- CCPA's private right of action and how it may mimic the current TCPA and BIPA litigation landscape
- Pending CCPA-like state laws that include private rights of action
- An overview of common information security safeguard standards that may be used to assess "reasonableness"
- Practical steps to take now to address and mitigate potential risks, including through reviewing and revising commercial contracts

Breach Notification in California

WINSTON & STRAWN LLP

Existing California Breach Requirements

- California requires notification to individuals whose personal information is breached
  - Personal information defined as a person's name combined with several data elements, such as:
    - Government ID (e.g., SSN)
    - Financial account number (e.g., credit card number)
    - Electronic username and password (e.g., email account)
    - Medical information
- Notification required to Attorney General if more than 500 CA residents affected

How Does the CCPA Interact with the CA Breach Notification Statute?

- The CCPA's private right of action is tied to the existing CA breach notification law
- Allows individuals whose non-encrypted personal information, as defined by CA's breach law, to bring suit
- The existing breach law uses a much narrower definition of personal information than CCPA
- What about HIPAA- and GLBA-covered entities that have partial exemptions from CCPA requirements?

The CCPA's Private Right of Action

WINSTON & STRAWN LLP

The CCPA's Private Right of Action

- There is a private right of action for data breaches for info protected under existing CA breach notification law
  - Failure to implement "reasonable" security procedures and practices to protect information
  - Must provide opportunity to "cure"
  - Consumers may seek the higher of actual damages or up to $750 per incident
  - This private right of action applies to employee data
- Availability of statutory damages likely to increase class action
  - Data breaches typically face limited class action interest outside of the biggest breaches
  - It is difficult to prove actual damages

Dissecting the Private Right of Action

- **What Information?** *"Personal information" as defined in California's breach notification law*

- **Who has the right to bring an action?** *Any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information*

Dissecting the Private Right of Action

- **Where does that duty come from?** *Cal. Civ. Code 1798.81.5(b)"A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."*
- **When can someone bring an action?** *Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer shall provide a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated.*

Dissecting the Private Right of Action

- **… But there's a cure period, right?** *In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.*

- **What does that mean?** *In practice, probably not. Once the information has been accessed and exfiltrated, subject to theft, or disclosed, it'll be difficult to argue that a cure is possible.*

How Does This Change Existing Breach Lawsuits?

- Under current law, data breach class actions are generally limited to large-scale breaches
  - Plaintiffs' bar is wary of bringing breach claims because plaintiffs often struggle to show actual harm
  - Thus, these complaints are often dismissed for lack of standing
- The availability of statutory damages removes the argument that plaintiffs are not "harmed" by violations of the law
- Likely that all breaches involving CA residents will result in a class action complaint after January 1, 2020

Lessons From Similar Laws: BIPA and TCPA

- The CCPA combines a private right of action (for security breaches) with statutory damages
- This combination has proved a boon for plaintiffs' attorneys in two similar consumer privacy laws:
  - The federal Telephone Consumer Protection Act (TCPA) and
  - Illinois' Biometric Information Privacy Act (BIPA)
- Hundreds of class actions filed a year under these "gotcha" statutes

Going Beyond the CCPA

WINSTON & STRAWN LLP

CCPA Copycats that Go Beyond the CCPA

- A number of states have proposed identical bills to the CCPA
  - None made it out of committee in the spring legislative session
- New York Privacy Act –
  - Requires opt-in consent before processing consumer data,
  - Places a fiduciary duty on businesses processing consumer data, and
  - Contains a global private right of action
- Massachusetts S. 120 – Contains a general private right of action

Others Laws to Monitor

- Several states considering sector-specific privacy laws, including those regulating:
  - Biometric information;
  - Financial services;
  - Online privacy; and
  - Student privacy
- In addition, there are several pending federal privacy bills, including first-of-their-kind federal privacy bills

What is Reasonable? Common Safeguard Standards

WINSTON & STRAWN LLP

The Reasonableness Standard

- Other data security laws use similar language. For instance:
  - GDPR
  - FTC – Privacy by Design
  - State laws – How is reasonableness enforced and interpreted?
- Federal Trade Commission
  - *LabMD v. Federal Trade Commission* – 11th Circuit refused to enforce FTC order require implementation of a reasonable security program because the standard was "vague"
  - In other FTC enforcement cases, specific types of safeguards are discussed

The Reasonableness Standard (cont.)

- In *Federal Trade Commission v. Wyndham Worldwide Corporation*, the Third Circuit found that Wyndham's security was unreasonable
- In reaching this conclusion, the court drew comparisons against the 2005 Card System Solutions Breach:

CSS	Wyndham
Stored PII in a vulnerable format for 30 days	Stored card payment information in a readable format
Did not test against commonly known threats despite readily available defenses	Failed to monitor the network for the same malware used in a previous breach
Weak passwords	No minimum password requirements
Weak access controls and firewalls	Weak access controls and firewalls
Failure to sufficiently monitor the network for attacks	Failure to sufficiently monitor the network for attacks

Laws that Enumerate Specific Standards

- State laws (most notably, Massachusetts and Nevada)
- HIPAA (50+ required and addressable specifications)
- Gram-Leach-Bliley Act (for financial institutions)
- New York Department of Financial Services Cybersecurity Regulation (for financial institutions)

Common Industry Safeguard Standards

- There are several common industry and government security standards, including standards published by:
  - National Institute of Standards and Technology (NIST)
  - Center for Internet Security (CIS)
    - This is of particular interest with respect to CCPA, given comments in 2016 by then-CA Attorney General Kamala Harris, but has not been blessed by current CA Attorney General Xavier Becerra
  - International Organization for Standardization and International Electrotechnical Commission (ISO/IEC)

Common Industry Safeguard Standards

- In 2016, pre-CCPA, Attorney General Harris released a breach report, analyzing breaches from 2012-2015
- In this report, the AG discussed various breach trends
- Also endorsed the CIS' Critical Security Controls, a set of 20 different data security safeguards
  - AG noted that these controls establish the minimum level of security for organizations, and failure to comply would be a "lack of reasonable security"
- The controls include various technical, organizational, and administrative safety measures, including:
  - Inventory and control over hardware and software;
  - Continuous vulnerability management;
  - Access privileges;
  - Secure laptops and mobile devices;
  - Maintenance and monitoring of audit logs;
  - Email and web browser protections

So How Can CCPA Covered Entities Be "Reasonable"

- Unfortunate answer: we don't know for sure
- Will be a fact-dependent (and likely, litigation-driven) exercise
  - A sliding scale depending on the size of the organization and the amount/type of data at issue
- However, organizations can take steps to put themselves in the best position possible, including:
  - Implementing security oversight
  - Certifying with one or more of the cybersecurity standards
  - Addressing the 20 CIS standards
  - Focusing on encrypting sensitive data, where possible
  - Implementing an enterprise-wide written information security program
  - Conducting regular security audits, including penetration testing
  - Training employees and raising awareness
  - Practicing data minimization
  - Staying on top of security trends

Practical Steps to Take Now to Mitigate Risk

WINSTON & STRAWN LLP

Implement Vendor Oversight

- Once you map out which third-party organizations have your sensitive data, review these agreements to understand whether current contractual provisions are sufficient, given CCPA's private right of action
- Look at key terms, including:
  - Indemnification
  - Limitation of liability
  - Exclusion of certain damages
  - Scope of the agreement (e.g., do you have to worry about CCPA and GDPR?)

Implement Vendor Oversight

- Initial Assessments
  - How are you vetting your vendors?
  - Are you vendors able to comply with shifting privacy laws and developing threats?
  - Where feasible, do you obtain any documentation up-front regarding the vendor's security posture?
  - Have your vendors had any recent security incidents?
  - Do you have an effective commercial contracting process in place (e.g., so your organization can ensure that all contracts affecting sensitive personal data undergo an appropriate review/vetting process)

Implement Vendor Oversight

- Data Security Terms
  - Does the vendor include baseline safeguards?
  - How are vendors disposing of data?
  - Do you have approval rights over the use of subcontractors?
  - Do you have audit rights? What do they look like?
  - Can the vendor update its DPA or data security terms without notice?
  - What are the notification requirements in the event of a security incident?
  - Do you have termination rights in connection with data security violations?

If You are the Vendor…

- You are in the hot seat for data security
  - Do you have sufficient insurance?
  - Do you track your customer data security requirements?
  - Have you updated your data processing addendums?
  - How do you monitor changes in data privacy and security laws?
  - Who in your organization provides oversight of your security program?
  - Have you reviewed your incident response plan?
  - What kind of oversight do you have over subcontractors?

Do Your Diligence

- Understand where your sensitive data “lives”
  - Conduct a data-mapping exercise to track how this information flows into, through and out of your organization
- Dispose of unnecessary data – and make sure your vendors do, too
- Talk to your business teams
  - What are they doing with personal information today, tomorrow and two years from now, and will your current security infrastructure be suffcient?
- Assess current data security
  - Undergo an audit, certification, and/or penetration testing
  - Identity gaps where controls are missing or outdated

Make a Remediation Plan

- You need to understand:
  - What data you have
  - What your organization plans to do with it
  - How it is protected
- Then, implement additional controls as necessary to meet best practice recommendations or established frameworks (e.g., NIST, CIS)
- Create a written plan to outline how the organization plans to address any security gaps or justify any implementation decisions (e.g., because the control is infeasible or too expensive)
- This assessment may become part of a defense in the event of a data breach class action in 2020 and beyond

Execute

- Take steps to ensure that there is oversight as to the remediation plan (e.g., who is in charge of updating it?)
- Data security is a team effort; do your employees know what their obligations are?
- Be creative in how you approach data security; it is important to meet baseline (e.g., “reasonable”) expectations, but you may need to come up with new security solutions based to address dynamic products and services
- Encourage communication between the marketing, product, human resources, security and legal teams
- Ensure that there is a vendor oversight process in place

Thank You!

Sean Wieber
Partner
Chicago
(312) 558-5769
swieber@winston.com

Becky Troutman
Partner
San Francisco
(415) 591-1401
btroutman@winston.com

Alessandra Swanson
Of Counsel
Chicago
(312) 558-7435
aswanson@winston.com

Eric Shinabarger
Associate
Chicago
(312) 558-8823
eshinabarger@winston.com