
IFA
INTERNATIONAL FRANCHISE ASSOCIATION
FRANCHISE LAW
VIRTUAL SUMMIT
August 12-13, 2020

Introductions

Heather Buchta
Quarles & Brady

Liz Harding
Polsinelli

Paul Luehr
Faegre Drinker Biddle & Reath

Agenda

- **Today's Context – Quickly Changing**
- **Practical Implications**
  - Tools
  - Negotiations
- **Enforcement Implications**

Privacy Landscape 2020

- **California**
- **Europe**

Privacy Landscape

- **Hotel California**
  - Effective January 1, 2020
  - Enforcement July 1, 2020
  - Regulations are not yet finalized

Status of Regulatory Enforcement

- **Proposed Regulations sent to OAL June 1, 2020 in advance of July 1, 2020 enforcement date**
- **OAL has announced that it has 120 days from July 16, 2020 to review**

Procession of Draft Regulations

- **Not much change from original draft**
- **Questions remain**
  - IP addresses as identifiers?
  - Potential overreaching in regs?

Substance of the Regulations

- **Rights Verification and Submission Process**
  - Website processes
  - Database coordination
- **Notices at Collection**
  - Website
  - In-Person
  - Telephone

California Saga – Part 2

- **California Privacy Rights and Enforcement Act of 2020**
- **Qualified for November 2020 ballot**
- **Expected to Pass**

Implications of CPRA
The Good News

- **B2B/E'ee Exceptions**
  - Extended until 2023
- **Cleans up some definitions and ambiguities**

Implications of CPRA
The Bad News

- **Lots of new concepts**
  - Sensitive PI Obligations
  - Additional Consumer Rights
  - Additional Contracting Obligations
  - Reinstates the Technical Sale Opt-Out
  - Establishes New Administrative Agency

And in Other News....

- **Schrems II Decision issued July 16, 2020**
- **Struck down Privacy Shield as data transfer mechanism**
- **Adds layer of complexity to SCCs**

Vendor Interactions and Schrems II

- **New Focus on Transfer Mechanisms**
- **Individual Assessment –** in receipt of:
  - FISA subpoena or warrant?
  - National Security Letter ("NSL")

Vendor Interactions post-CCPA

- **Consumer Rights and Requests**
  - ✓ Right to Know
  - ✓ Right to Delete
  - ✓ Right to Opt-out of “Sale”

- **Franchises treat as “Brand” issue**
  - Franchise Agreement or Amendments
  - Operations Manual

Vendor Interactions post-CCPA

- **Facebook:** respond to DoNotSell requests
- **Terms:**
  - LDU = “Limited Data Use”
  - Pixel = code for individual/device (front-end)
  - API = “Application protocol interface” (back-end)
- **Timing**
  - July (Oct 20, 2020) “transition” – LDU applied to all CA traffic
  - Aug. 2020 – businesses must affirmatively select LDU

Source: https://www.facebook.com/business/help/1151133471911882

Vendor Interactions post-CCPA

Pixel

This site uses cookies. Some of them are essential, while others help us improve your experience.

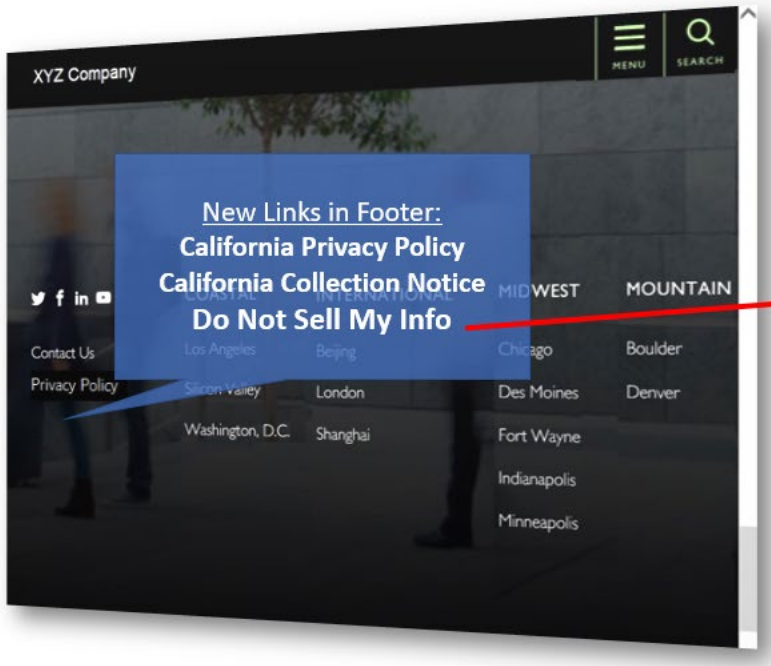
Policies | Details

Continue to site

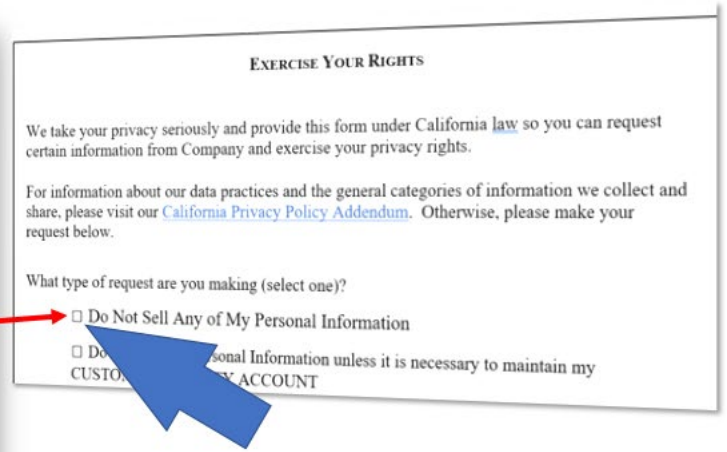
Do not sell my information

Cookie Banner

Home Page



Opt Out Page



EXERCISE YOUR RIGHTS

We take your privacy seriously and provide this form under California law so you can request certain information from Company and exercise your privacy rights.

For information about our data practices and the general categories of information we collect and share, please visit our California Privacy Policy Addendum. Otherwise, please make your request below.

What type of request are you making (select one)?

☐ Do Not Sell Any of My Personal Information

☐ Do sonal Information unless it is necessary to maintain my CUSTO ACCOUNT

Vendor Interactions post-CCPA

Set API:

App Events API [terms]

App Events via Facebook SDK [terms]

Audience Network Ad Request and Bidding via Audience Network SDK [terms]

Conversions API (formerly known as Server-Side API) [terms]

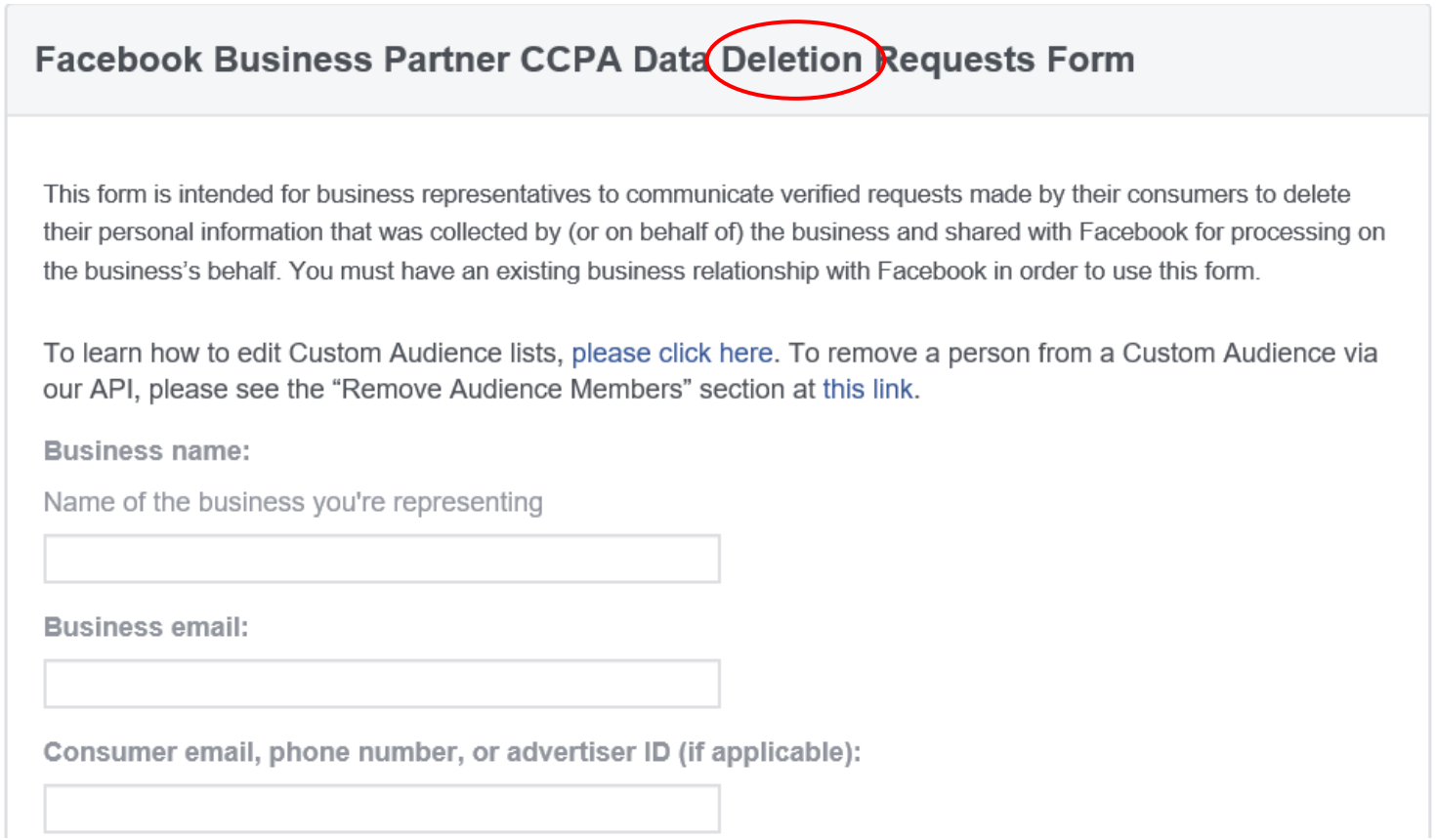
Facebook Pixel [terms]

Offline Conversions [terms]

Always on: Customer List Custom Audiences [terms] (July 1, 2020)

Source: https://www.facebook.com/legal/terms/state-specific

Vendor Interactions post-CCPA



Facebook Business Partner CCPA Data Deletion Requests Form

This form is intended for business representatives to communicate verified requests made by their consumers to delete their personal information that was collected by (or on behalf of) the business and shared with Facebook for processing on the business's behalf. You must have an existing business relationship with Facebook in order to use this form.

To learn how to edit Custom Audience lists, please click here. To remove a person from a Custom Audience via our API, please see the "Remove Audience Members" section at this link.

Business name:

Name of the business you're representing

Business email:

Consumer email, phone number, or advertiser ID (if applicable):

Source: https://www.facebook.com/help/contact/614340055979319

Vendor Interactions post-CCPA

- **Facebook – 3 options**
  - Send an email (“fire and forget”)
  - Use Facebook LDU
    - Withhold DoNotSell consumers from shared lists
    - Set LDU flag for individual DoNotSell requests (Leave global until Oct 20)
    - Report deletion requests
  - Use another CCPA management tool (e.g. IAB)

Vendor Interactions post-CCPA

- **Vendor Contracts**
  - CCPA – Addendum, Require Vendor to:
    - Retain, use or disclose Personal Information only for purpose under Agreement
    - Not sell, make available or otherwise disclose Personal Information to 3rd parties
    - Delete any Personal Information upon request
    - Certify it understands and will comply with these restrictions.
  - Other Negotiated Terms
    - Breach notice period
    - Information security requirements
    - Indemnification

Despite Delay – Enforcement Begins

- **First round of enforcement letters out July 1**
- **30-day remedy period concludes July 30**

First Round of Enforcement Actions

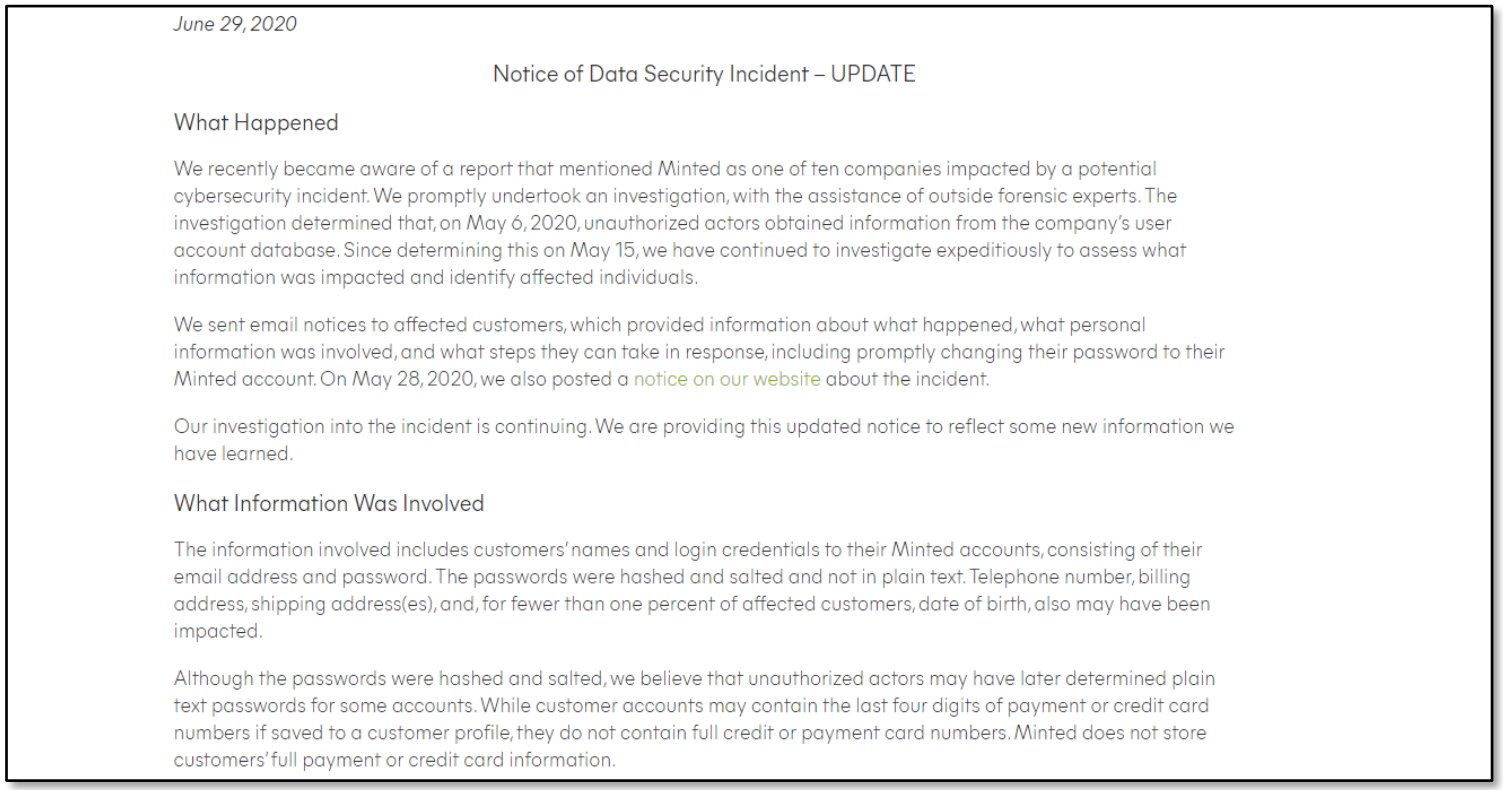
- **Not much information to date**
  - But initial round of enforcement letters sent targeting companies across all sectors.
  - Likely to focus on companies which have previously been the subject of consumer complaints regarding privacy issues.

Developments in the Private Right of Action under CCPA

- **Effective Date January 1, 2020**
- **Applies with respect to breaches impacting protected classifications of personal information (SSN, driver's license or California ID card number, account number or credit / debit card number, plus PIN or access code, medical or health insurance information).**
- **Allows recovery of the greater of (i) $100 - $750 per consumer per incident, or (ii) actual damages.**
- **Defense of reasonable security.**

Developments in Class Action (i)

- **Minted.com**



June 29, 2020

Notice of Data Security Incident – UPDATE

What Happened

We recently became aware of a report that mentioned Minted as one of ten companies impacted by a potential cybersecurity incident. We promptly undertook an investigation, with the assistance of outside forensic experts. The investigation determined that, on May 6, 2020, unauthorized actors obtained information from the company's user account database. Since determining this on May 15, we have continued to investigate expeditiously to assess what information was impacted and identify affected individuals.

We sent email notices to affected customers, which provided information about what happened, what personal information was involved, and what steps they can take in response, including promptly changing their password to their Minted account. On May 28, 2020, we also posted a notice on our website about the incident.

Our investigation into the incident is continuing. We are providing this updated notice to reflect some new information we have learned.

What Information Was Involved

The information involved includes customers' names and login credentials to their Minted accounts, consisting of their email address and password. The passwords were hashed and salted and not in plain text. Telephone number, billing address, shipping address(es), and, for fewer than one percent of affected customers, date of birth, also may have been impacted.

Although the passwords were hashed and salted, we believe that unauthorized actors may have later determined plain text passwords for some accounts. While customer accounts may contain the last four digits of payment or credit card numbers if saved to a customer profile, they do not contain full credit or payment card numbers. Minted does not store customers' full payment or credit card information.

Developments in Class Action (ii)

- **Epiq Systems**

Common themes…

- **Failure to implement reasonable security and to properly encrypt personal information.**
- **Broad interpretation of protected classifications of data (email address as account number, hashed password not encrypted).**

Complicating Factors

- **Capital One Decision**
  - IT forensic report not subject to legal professional privilege
- **Closer scrutiny to overall compliance**
  - Lister hospital
  - Back to Schrems – be careful about legal mechanism for transfers.

Questions