UPDATED

June 16, 2026

TO: Members, Assembly Privacy and Consumer Protection Committee

SUBJECT: SB 923 (BECKER) CONSUMER PRIVACY REQUESTS: DELETION REQUEST RECORDS AND REQUEST SUBMISSION METHODS
OPPOSE UNLESS AMENDED – AS AMENDED JUNE 11, 2026
SCHEDULED FOR HEARING – JUNE 23, 2026

The California Chamber of Commerce and the undersigned respectfully **OPPOSE UNLESS AMENDED SB 923 (Becker)** as amended June 11, 2026, because the bill fails to recognize that a business should also be deemed in compliance with a consumer's request to delete their data by opting the consumer out of processing for non-exempt purposes, in addition to retaining the minimum data necessary to honor the deletion request.

While the exemptions under Civil Code Sec. 1798.150 presumably apply, explicitly including this language provides clarity, particularly when this bill appears modeled upon other states like Virginia that have expressly adopted both limitations upon the right of deletion. From an operational and legal perspective, this language is essential to prevent confusion, to ensure technical scalability, and to allow businesses to fulfill obligations related to fraud prevention, security monitoring, and legal compliance.

First, without an opt-out mechanism, data received again from external sources like business partners could re-enter systems, requiring repeated deletions even if you do not further process (use, sell, disclose or share in any fashion) that information. In effect, this creates a "whack a mole" scenario, increasing the chances of accidental violations and significant compliance burdens, despite that fact that the consumer's data is as good as non-existent. Furthermore, large-scale deletion across distributed systems, logs, and backups is costly and operationally complex whereas an opt-out mechanism provides a scalable solution that ensures compliance with consumer rights in a practical and sustainable way.

Second, businesses must retain certain information for things such as fraud prevention, security monitoring, and compliance with other laws. Strict deletion requirements could be seen as conflicting with such obligations. Allowing companies to opt a consumer out of processing for non-exempt purposes enables them to retain only the necessary information about that consumer without using it for marketing, analytics, or other non-exempt activities. This limited retention is especially critical for fraud prevention, because data obtained "about the consumer" from third party sources—such as alerts about compromised credentials, suspicious account activity, or identity verification checks—can be used to detect, stop or mitigate fraudulent activity targeting that consumer. By keeping just enough information for these exempt purposes, companies can protect consumers from harm while respecting their privacy choices.

In short, without the opt-out provision, businesses would be legally obligated to delete data but practically unable to guarantee it remains deleted, creating operational inefficiency, compliance risk and increased costs for no real benefit to the consumer. Including this language is therefore critical to ensuring that **SB 923** is enforceable in a manner that protects consumer privacy while remaining feasible for businesses.

To address these concerns, we request the following change, as follows:

> 1798.105 (c) (1) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records, notify any service providers or contractors to delete the consumer's personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.
>
> *(2) A business that has obtained personal information about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete that data pursuant to subdivision (a) by* ***either (i)*** *retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal information remains deleted from the business's records and is not being used for any other purpose*, ***or (ii) opting the consumer out of the processing of such personal information for any purpose except for those exempted pursuant to the provisions of this title.***

Additionally, because of the difficulty relating to spam, many companies have transitioned to webforms or portals as a more reliable way to be contacted by consumers. Moreover, requiring businesses to publish an email address as the sole online method for receiving consumer requests poses significant cybersecurity concerns. Publicly available email addresses are routinely harvested by cybercriminals and used as vectors for phishing attacks, exposing companies to data breaches and operational disruption. This risk is substantially heightened today by the proliferation of AI-powered cyberattacks, which enable threat actors to generate highly convincing, targeted phishing communications at scale - making a static, publicly listed email address an increasingly dangerous point of vulnerability. Permitting businesses to use secure online methods such as webforms or portals mitigates these risks by providing controlled, authenticated channels that are far less susceptible to exploitation. To that end, we request this additional change:

> 1798.130 A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address ***or*** ~~***and***~~ *make an online method, such as a web form or online portal, available* for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

June 11 amendments fail to address concerns

Recent amendments add findings and declarations that appear intended to address the concerns raised in our opposition letter. However, those declarations merely restate the policy objective of extending deletion rights to personal information obtained from third parties and preserving existing statutory exemptions. They fail to address the central compliance issue raised by the bill: whether a business may satisfy a deletion request by maintaining a suppression record or otherwise opting a consumer out of future processing of third-party data.

Specifically, the findings acknowledge that businesses have legitimate security, integrity, fraud-prevention, and legal obligations that require retention of certain information. However, they do not recognize that businesses may also need to retain minimal information solely to ensure that deleted information is not reintroduced into their systems from third-party sources. Nor do they address the operational reality that, absent an express opt-out or suppression mechanism, the same consumer data may repeatedly flow into a business's systems from external sources, requiring recurring deletion requests and creating unnecessary compliance risk without providing any additional privacy benefit to the consumer.

Likewise, the findings' statement that consumers deserve control over their personal information regardless of source does not resolve how businesses should implement that control in practice.

While the findings acknowledge that businesses may retain information for certain exempt purposes, they do not explain how a business can both retain information necessary to satisfy those purposes and demonstrate compliance with a deletion request. Absent such direction, businesses are left with the uncertainty of either deleting information needed for fraud prevention, security, and legal compliance, or retaining that information and facing potential claims that the deletion request was not honored. The requested opt-out language resolves that ambiguity by making clear that a business remains compliant so long as it retains only the minimum information necessary for exempt purposes and refrains from processing the information for any non-exempt purpose.

It is important to note that the requested amendment would not diminish consumer rights; rather, it would provide a clear and scalable compliance pathway that prevents further processing of the consumer's information while allowing retention of only the minimum data necessary to honor the deletion request, prevent re-collection, combat fraud, maintain security, and comply with legal obligations.

In short, the findings explain why the Legislature wants deletion rights to apply to third-party data, but they do not address whether a suppression-list or opt-out approach should be deemed compliant with those rights. As a result, the findings leave unresolved the precise legal and operational concerns identified in our letter.

Moreover, even if the findings were intended to address those concerns, findings and declarations are not operative statutory language. While they may provide context regarding legislative intent, they do not establish a compliance standard, create a safe harbor, or specify how a business may satisfy its obligations under Section 1798.105. Thus, the uncertainty regarding whether retention of limited information for suppression, fraud-prevention, security, or legal-compliance purposes is consistent with a consumer's deletion request would remain. Businesses are ultimately governed by the substantive requirements of Section 1798.105, not the bill's findings and declarations. Accordingly, if the Legislature intends to permit businesses to retain minimal suppression records or satisfy deletion requests through an opt-out mechanism for non-exempt processing, that direction should be reflected in the operative provisions of the statute.

For these reasons, however, we must **OPPOSE UNLESS AMENDED SB 923 (Becker).**

Sincerely,

Ronak Daylami
Vice President for Advocacy | Privacy, Cybersecurity & Emerging Technologies
on behalf of

American Car Rental Association, Don Lefeve
Association of National Advertisers, Christopher Oswald
California Bankers Association, Chris Schultz
California Chamber of Commerce, Ronak Daylami
California Restaurant Association, Matt Sutton
Civil Justice Association of California, Annalee Augustine
Computer & Communications Industry Association, Aodhan Downey
Insights Association, Howard Fienberg
Silicon Valley Leadership Group, Ahmad Thomas
Software Information Industry Association, Abigail Wilson
TechCA, Courtney Jensen
TechNet, Robert Boykin

cc: Legislative Affairs, Office of the Governor
Gilbert Martinez, Office of Senator Becker
Consultant, Assembly Privacy and Consumer Protection Committee
Liz Enea, Consultant Assembly Republican Caucus

RD:ldl