Published on *The National Law Review* https://natlawreview.com

Analysis of Modified Attorney General Regulations to CCPA—Part 3: Verification of Requests

Article By:

Natalie A. Prescott

Cynthia J. Larose

I. Overview:

In this post, we offer insights on the revisions recently made by the California Attorney General's office to Article 4 of its draft regulations pertaining to verification requirements. Article 4 specifies how businesses should verify consumers' identities when they receive consumers' data requests. We previously reported on this part of the draft regulations here. In addition to explaining the key changes, we again offer our recommendations and summarize the elements of the draft regulations in their latest form.

Here is an overview of the most prominent revisions:

- Businesses may not require the consumer to pay a fee in connection with verifying the consumer's identity when the consumer makes a request to know or to delete.
- For example, the business cannot require a notarized affidavit from the consumer, unless the business reimburses the consumer for those costs.
- For non-accountholders, if a business chooses to require signed declarations from its consumers, those collected declarations must be maintained as a part of the business's record-keeping obligations.
- For non-accountholders, a new example is provided to explain the type of information that necessitates verification with "only" a reasonable degree of certainty: If a retailer maintains a record of consumer's purchase history, verification to a reasonable degree of certainly requires only asking the consumer to identify the items they purchased or the dollar amounts of the most recent purchase.
- In discussing non-accountholders, the revised draft regulations delete the confusing phrase, "fact based verification process" and now explain that, when the business's mobile app collects information but does not require consumers to set up accounts, the business should

consider the factors set forth in section 999.323(b)(3) to help it decide whether it may reasonably verify a consumer either (1) by asking about information that only the person who used the mobile app would know or (2) by having the consumer respond to a notification sent to their device.

- For non-accountholders, the business can now deny the consumer's request to know specific personal information if the business is unable to verify the requestor's identity.

- If the business has no reasonable method for verifying the consumer's identity to the requisite degree of certainty for non-accountholders, it now must explain it its privacy policy why it has no such method. Furthermore, it must document on a yearly basis whether a reasonable verification method can be established.

- The business can now require that the authorized agent making a request on consumer's behalf must provide both written and signed permission from the consumer.

- The business is now allowed to directly confirm with the consumer that they had, in fact, authorized an agent to make requests on their behalf.

- Two new obligations are added for authorized agents making requests on behalf of consumers: (1) they must implement and maintain reasonable security procedures and practices to protect the information; (2) they may not use any information collected from or about the consumer for any purpose other than to fulfill the consumer's requests, for verification, or for fraud prevention.

II. **Our Top 10 Recommendations:**

Generally speaking, businesses must (i) verify consumers' requests by using available data and implementing reasonable security measures, (ii) not collect new data for verification unless absolutely necessary, and (iii) promptly delete newly collected information. Notably, businesses do not have to re-identify data or provide or delete deidentified information. Additional requirements apply to password-protected accounts and to non-accountholders, as discussed below. On the consumer side, consumers may use authorized agents to make requests on their behalf, but the additional hurdles seem to discourage this procedure.

We recommend the following steps to help businesses comply with the newly revised verification guidelines:

1. Deidentify as much data as possible.

2. For data that cannot be deidentified, create a verification mechanism that addresses the specific categories of data and how it should be used for verification.

3. Train employees on how to respond to and how to verify consumer requests.

4. Apply a layered approach to verification: The more sensitive the data, the more stringent the procedure must be.

5. Create a protocol for documenting compliance with these regulations.

6. Create a protocol for and train employees on when it is appropriate to collect “new” data from the consumers, when not to collect new data, how to store it, and how to delete it in a timely manner.

7. Interview and select a highly reputable vendor, if appropriate, for purposes of complying with the verification requirements.

8. Exercise special care when accepting verification requests from non-accountholders.

9. Watch out for fraud and maintain reasonable security measures.

10. Avoid charging consumers any fees in connection with verification or reimburse for fees.

III. **Key Verification Requirements:**

Section 999.323 of the draft regulations requires businesses to do the following:

1. **Verify** that the person making a request is the actual consumer.

2. **Document business’s compliance** with the verification requirements.

3. Create a **reasonable method** for verification.

4. Account for the possibility of **fraudulent requests.**

5. Maintain **reasonable security measures** to detect fraud and prevent unauthorized access.

6. For **more sensitive information**, follow a more stringent verification process.

7. For information that carriers a **greater the risk of harm** to the consumer if it is misappropriated, utilize a more stringent verification.

8. For information that is **more likely to be misappropriated**, follow a more stringent verification process.

9. **Match the information the business already has** to the information the consumer provides, whenever feasible (using a third-party verification-service is permissible for these purposes).

10. **Avoid collecting new information**, unless absolutely necessary for verification purposes.

11. **Delete newly collected information** as soon as practical (unless it is still needed for compliance with the 24-months-record-keeping requirements in section 999.317).

12. **Not require a consumer to incur fees** or expenses in connection with verification (including notarizing documents), unless the business compensates the consumer.

IV. **Verification for Password-Protected Accounts:**

Section 999.324 sets forth separate requirements for password-protected accounts.

1. If a consumer has a password-protected account on the business's website, the business can use its existing authentication practices, such as two-factor authentication, to verify that consumer's identity.

2. Consumers **must re-authenticate** themselves before their data is disclosed or deleted.

3. If a business **suspects fraud, it shall not comply** with the consumer's request until it determines via further verification procedures that the request is authentic. Procedures set forth in Section 999.325 may be used for these purposes.

V. **Verification for Non-Accountholders:**

Section 999.325 outlines the more stringent verification steps, which apply to non-accountholders. If the consumer does not have or cannot access their password-protected account, the business must comply with both, Section 999.323 outlined above and with the additional requirements laid out in Section 999.325, below. If a business has no reasonable method by which it can verify the consumer's identity, it must state so in its response, explain the reasons in its privacy policy, and re-visit and document this issue annually.

1. Request to Know Categories of Personal Information: The business must verify the consumer's identity "to a **reasonable degree** of certainty." For example, the business can match at least two reliable data points.

2. Request to Know Specific Pieces of Personal Information: The business must verify the consumer's identity "to a **reasonably high degree** of certainty." For example, the business can match at least three reliable data points, plus obtain a **signed declaration** under the penalty of perjury that the requestor is the consumer (and then maintain all declarations pursuant to its record-keeping obligations).

3. Request to Delete: Depending on the sensitivity of the information and the risk of harm, the business must verify the consumer's identity either "to a reasonable degree or a reasonably high degree of certainty."

    a. Examples of deletion requests that require a high degree of certainty:

        i. Family photos.

        ii. Family documents.

    b. Examples of deletion requests that require only a reasonable degree of certainty:

        i. Browsing history.

ii. Purchase history.

4. Request to Know Specific Pieces of Personal Information: The business must deny such requests if it cannot properly verify the requestor's identity.

VI. When a Consumer Uses an Authorized Agent for Verification:

Section 999.326 permits consumers to use authorized agents to make requests on their behalf, but it then allows the businesses to ask for more documentation.

1. If a consumer uses an authorized agent to make a request on his or her behalf, the business may require either a written and signed permission from the consumer or a direct contact between the consumer and the business.

2. The business can deny a request from the agent, if it deems the proof or authorization to be insufficient.

3. An authorized agent must implement and maintain reasonable security procedures and practices to protect consumer's information.

4. An authorized agent cannot use the consumer's information for any other purpose.

VII. Takeaways:

In verifying the consumer's identity, businesses must first set up and then carefully document their verification process. The AG's solution in the revised draft regulations is that businesses should match the categories of information the consumer provides with the information businesses already have. As such, the draft regulations advise against collecting additional information for verification, unless doing so is absolutely necessary. Additionally, businesses should not charge fees or cause consumers to incur unreimbursed expenses in connection with verification.

Businesses can also use third-party verification systems for verification purposes and do not have to provide, delete, or re-identify data that has been deidentified. Unless absolutely necessary, businesses should not collect highly sensitive information such as social security numbers, driver's license numbers, and other sensitive data. In short, businesses must simply match the consumer's data with the data they have on file; collect new data only if necessary; implement reasonable security measures; and keep consumers informed and safe from fraud.

Consumers may rely on third-party agents to make requests on their behalf. However, businesses have the right to refuse to cooperate with the agents if they reasonably deem the request to be unsafe, unverified, or non-compliant.

Read Part 2: Business Practices for Handling Consumer Requests and Part 1.

National Law Review, Volumess X, Number 50