IDOLOGY
a GBG company

Research Paper

CCPA and Identity Verification

Converting the Fulfillment of Verifiable Consumer Requests From a Complicated Mandate to a Competitive Differentiator

The California Consumer Privacy Act (CCPA) should not be viewed as a mere compliance exercise for California customers.

There are significant risks and opportunities, especially as the Act relates to the critical step of identity verification. The possible fines from the State of California are dwarfed by costly potential consumer lawsuits. CCPA also opens doors for fraudsters. Consumers will continue to expect the seamless, fast experiences leading firms provide, along with the right amount of friction in a myriad of channels and use cases.

Firms that provide a secure, efficient, and user friendly method of verifying the identities of CCPA requestors will be positioned well to comply with regulations, deter fraudsters, reduce costs, and attract customers.

Overview

Read this paper to find out the top four ways CCPA identity verification could become a competitive differentiator or a business fiasco.

1. Why identity verification is critical to the success of a CCPA compliance program
2. How the creation of a new threat vector impacts criminals and fraud
3. How CCPA may generate operational inefficiencies
4. How fostering customer engagement is vital during the moment of trust when a customer voluntarily submits a data request

Overview

January 1, 2020 (when CCPA goes into effect) and July 1, 2020 (California enforcement) are not finish lines; they are starting points. CCPA will have enormously long tails and more than likely will be nationalized, if not globalized. Verifying the identities of requesting customers is a fundamental imperative and crucial step to ensuring compliance and security while boosting customer trust.

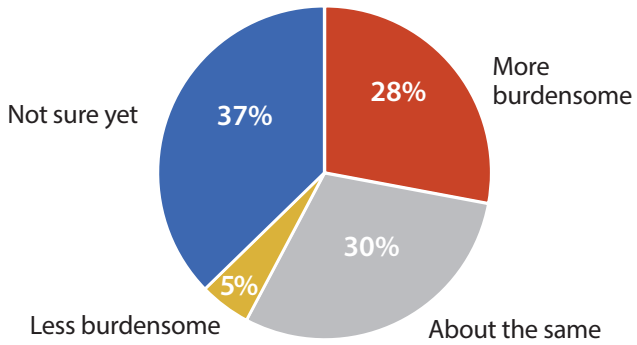
Defining the CCPA Identity Verification Business Problem: How to maintain compliance and give verified requestor access to personally identifiable data in an automated, secure, scalable, and self-service way that also facilitates a positive user experience and builds trust.

A Seismic Shift in the Compliance and Identity Verification Landscape

On the heels of the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act is the latest regulation to address the perceived imbalance in power that exists between companies and consumers when it comes to data management. Regardless of whether the organizations covered by CCPA can comply, the regulation will take effect in January 2020, with enforcement beginning in July 2020.

CCPA Differs from GDPR in Some Key Areas, Notably Identity Verification Processes

Compared to GDPR, what compliance burden will CCPA have on your organization?



Source: Seventh Annual Fraud Survey, IDology, 2019

One of the most challenging and complex issues associated with CCPA relates to identity verification. At its heart, CCPA requires affected businesses to provide Californians with access to the personal information held on them by a company. To do so, businesses must engage in identity verification (IDV).

Successful IDV for verifiable consumer requests is important for several reasons:

- Effective, well-designed IDV is vital for compliance with CCPA
- Strong IDV processes deter fraud
- Flexible, automated, and scalable IDV helps manage operational costs
- Clunky IDV with unreasonable friction negatively impacts both the customer experience and the brand

"There is a growing campaign by the plaintiffs' bar to target data privacy and security in the hopes of striking it rich in a new goldmine on the level of the asbestos litigation of the 1970s, 1980s, and 1990s."

The US Chamber of Commerce

CCPA gives CA residents the right to:

- Know what personal information is being collected about them
- Know whether and how their personal data is sold or disclosed and to whom
- Prohibit the sale of their personal data
- Request access to their personal data online or by phone or email

CCPA Penalties

Per Violation Fines:

$2,500 per violation for unintentional and $7,500 for intentional violations

Consumer Right of Action:

$100-$750+ per violation, per consumer, or actual damages, if higher for damage caused when non-encrypted or non-redacted personal information is breached.

The CCPA Identity Verification Baseline

California Attorney General Xavier Bacerra considered and ultimately rejected a plan to enforce one identity verification method for all businesses. With this decision, AG Bacerra provided flexibility to industries with different needs and use cases. Physical retail outlets, for example, may need to offer in-store personal data request forms; companies that operate solely online will not be required to offer a toll-free phone number for data requests. AG Bacerra's bias toward flexibility leaves the door open for future modifications as the security, fraud, and technology industries change.

Identity verification is, in fact, the linchpin for CCPA, and the process includes the initial intake request, security automation, and the ability to scale and maintain consumer engagement at a vulnerable time in the customer-business relationship. Although IDV methods have been around for a long time, they are increasingly complex, multi-dimensional, and multi-channel and are extremely important to customer onboarding, servicing, and security.

IDV for CCPA comprises two core elements. The first is the ability of the IDV process to vary verification thresholds and requirements based on the nature of the request and the sensitivity of the data requested (e.g., a straightforward data share request versus a data deletion request). Requests for data deletion or that involve sensitive information, such as health records, should require a stronger means of IDV.

The second core element of CCPA IDV involves the account status of the requestor. Some data requests will come from users with registered, password-protected accounts, while others will be submitted by users who do not have existing accounts. CCPA regulations stipulate that Californians are not required to have an online account to exercise their rights, nor can they be forced to create one. These details surrounding account creation have significant implications with respect to available data request channels and verification methods. Depending on how customers typically interact with a business, that organization may be required to accept data requests in person and via email, postal mail, and phone.

Organizations that will be well positioned to complete CCPA-related requests are those that understand the facets of CCPA identity verification and adopt IDV systems that scale and automate, are secure and easily integrated, and have multiple IDV methods that will satisfy consumer needs. However, that also requires enough security to detect and deter fraudulent requests and the ability to match the IDV method to the sensitivity of the data that that the consumer requested.

Gathering data and assessing its sensitivity level, the nature of the request, and the account status of the requestor is a complex process with hundreds of potential combinations of request types, channels, sensitivity levels, and requestor account statuses. Nonetheless, companies must be prepared.

An important part of CCPA IDV is the use of multi-factor authentication and matching criteria. Even with a registered password-protected online account, data requestors will need to reauthenticate themselves using a two-factor

Estimates suggest a total of **$467 million to $16,454 million in costs** to comply with CCPA 2020-2030.

Berkeley Economic Advising and Research, LLC, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations

"A business shall not at any time disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers."

California Attorney General Publishes Proposed CCPA Regulations

CCPA draft rules enable businesses to use the personal information they have on their requesting customer or use a third-party identity verification service to service requests.

"A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information".

California Attorney General Publishes Proposed CCPA Regulations

authentication process, such as a one-time mobile passcode. Some cases, depending on the sensitivity of the data and the method by which the request was submitted, will require businesses to verify three forms of identity.

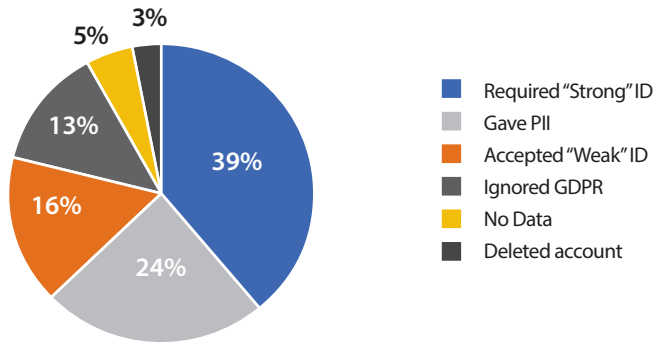
If the requestor's identity cannot be confirmed on the first submission, AG Bacerra's proposed regulations grant businesses the ability to "step up" or escalate to additional verification methods. Any additional information collected can only be used for identity authentication, security, or fraud prevention and must be deleted immediately after the requestor's identity has been verified.

If these stepped up verification methods fail to return a result, the company must alert the requestor, in writing, to the reason for the failure. An IDV system that uses transparent reason codes for IDV failures will make the process of handling verification issues much easier. This type of transparency will also facilitate intelligent dynamic escalation to other workable methods of identity verification if needed.

CCPA and Fraud Security: Learning from a GDPR Fraud Experiment

If GDPR is an indicator of how CCPA will unfold, then businesses need to consider how criminals can and will exploit subject access requests. An experiment featured in a Black Hat USA white paper by an Oxford University researcher and a security consultant demonstrates how easy it is to acquire personal information, thus exploiting the weak GDPR identity verification in many firms. The research conducted by James Pavur and Casey Knerr found that among 150 businesses tested for their ability to detect fraudulent document requests, many failed to adequately verify the identity of the requestor. The test was designed to replicate a fraudster's attack through subject access requests. Security consultant Casey Knerr played the role of the victim. Researcher James Pavur sent subject access requests in Knerr's name but without her participation or involvement. When organizations requested additional information to complete the requests, a small amount of publicly available information was provided in return.

Responses of Organizations That Received Malicious Subject Access Requests



Source: GDPArrrrr: Using Privacy Laws to Steal Identities; Black Hat USA 2019 white paper, James Pavur and Casey Knerr

Determining Costs to Verify Requests

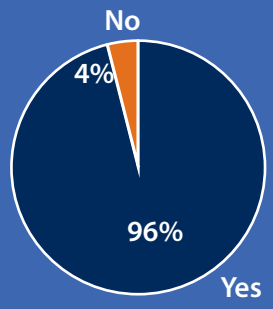
Number of California consumers doing business with the firm

- X % of consumers without an account
- X % of consumers making a CCPA request
- X incremental cost /person of verification
- = **Cost per firm**

Source: State of CA Department of Justice and Berkeley Economic Advising and Research

Identity Verification is Considered a Strategic Differentiator

Can identity verification be a strategic differentiator?



Source: Seventh Annual Fraud Survey, IDology, 2019

Best Practices Case Study: Microsoft

In response to GDPR, Microsoft successfully launched its global privacy self-service portal. In the first year, it received 18 million requests, 37% of which came from the U.S.

Source: Gartner

CCPA Compliance Does Not Equal CCPA Security

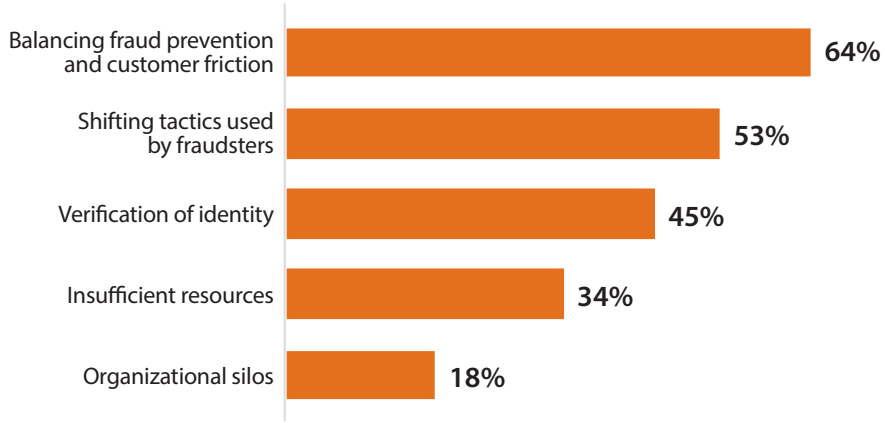
The results were troubling and illuminate the need for strong identity verification practices:

- Among the 150 companies, 72 replied to the fake requests with 83 companies affirming that they had information on Knerr.
- Alarmingly, 24% simply accepted an email address and phone number as proof of identity and sent over any files they had on Knerr to Pavur.
- Another 16% requested easily forged ID information.

The implication is that fraudsters can and will exploit weak CCPA subject rights request processes in large-scale ways to access sensitive personal information.

CCPA's Fraud Balancing Act: Make Access Easy for Customers While Deterring Fraudsters

What do you think are the biggest challenges to fraud deterrence within your industry? (Select all that apply)



Source: Seventh Annual Fraud Report, IDology, 2019

While CCPA is the latest regulation to put the power in consumers' hands, it certainly will not be the last, with numerous regulations undergoing review across the United States and around the world. Some would argue we've already entered a new era of consumer empowerment, with GDPR and CCPA being the first of many laws designed to put the consumer in the data privacy driver's seat.

Top CCPA Identity Verification Request Methods and Channels

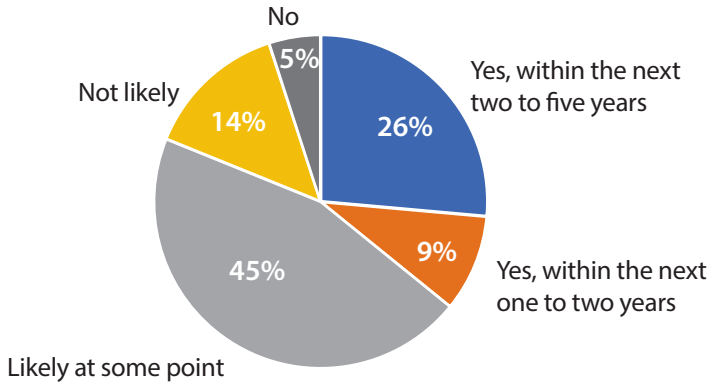
- Online User Name and Password
- Phone CSR Call Center
- Knowledge-Based Authentication
- Mobile One-Time Passcode Verification
- Mobile ID Scan
- Email Request and Verification

Businesses should vary the verification thresholds and requirements based on the sensitivity of the data requested and whether the request made is to share the data versus delete the data, with the latter requiring higher levels of verification.

California Attorney General Publishes Proposed CCPA Regulations

Majority of Businesses Believe CCPA Will Become National Law

Do you think CCPA's principles, such as requesting access to personal information, will ultimately be adopted nationwide (i.e., federal law)?



Source: Second Annual Consumer Digital Identity Survey, IDology, 2019

Verifiable Consumer Requests Under CCPA

CCPA allows California consumers to compel covered organizations to disclose certain facts about the consumer data they possess. To trigger this request, the consumer must submit a verifiable consumer request (VCR), also known as a subject's rights request.

"'Verifiable consumer request' means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify."

Source: AB-375, California Consumer Privacy Act, 2018

While a VCR is a compliance mandate, complying with a request presents a complicated challenge. CCPA in its current form includes some limitations on how a company can administer identity verification. For example, to fulfill a request, a company cannot mandate the creation of a user account. That's particularly challenging as it compels a company to validate a VCR without data it would normally have in its possession associated with an authorized account.

Also, aside from internet-only companies, all other firms must accept requests over the phone as well as via traditional channels. This differs from GDPR, which only allows requests via email, fax, or letter. Organizations cannot make the process too difficult by requesting excessive amounts of data from the consumer. They cannot require the submission of more sensitive data than the consumer wishes to request, and the organization receiving the request must process it within 45 days of its receipt. The request can cover the past 12 months and must be provided in a transferable manner.

"Personal information" is anything that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Data attributes include names, addresses, SSNs, email addresses, geolocation, IP addresses, shopping or browsing history, psychological profiles, behaviors, attitudes, consumption behaviors, and consumer preferences.

"Whereas many organizations may be focusing on the fines or the litigation, subject rights requests left unmanaged have the potential of becoming 'death by a thousand cuts' and costing the organization millions of dollars on an ongoing basis."

Gartner

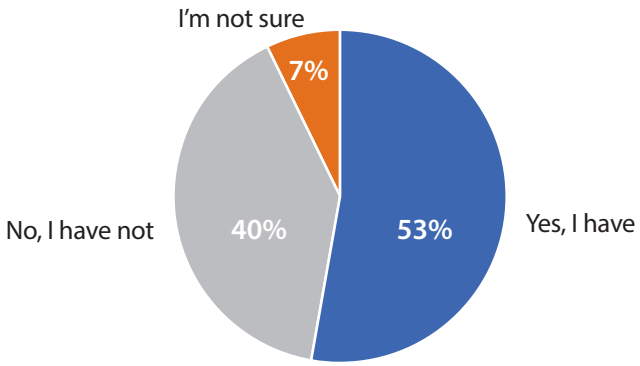
By 2021, 80% of the negative financial impact of CCPA will come from failure to implement a scalable subject rights workflow, as opposed to regulatory fines and litigation.

Gartner

VCRs under CCPA are new to consumers, though identity verification processes are not. There is data on IDV practices and escalation methods and their impact on trust and company preferences. Because VCRs are new to consumers, their expectations regarding the ease and speed with which companies fulfill these requests may initially exceed organizations' abilities.

Majority of Consumers Have Experienced "Step Up" Identity Verification Using Multiple Methods

In the last 12 months, have you been required to provide further proof of your identity while signing up for a new online account or using an existing online account? This could include answering personal questions or submitting identification documents.



Source: Second Annual Consumer Digital Identity Survey, IDology, 2019

When a consumer requests their information on file, it's a moment of vulnerability, similar to asking a stranger for their first impressions of you. Not disclosing the information quickly enough can create angst and distrust. Undoubtedly, expectations will evolve as more companies fulfill requests and consumers see how long it takes to fulfill them. With that said, organizations with a well-designed process will set the bar for others to clear.

Creating a Competitive Differentiator; More Secure, Less Expensive, Superior Experience

To fulfill VCRs, organizations must possess the ability to vet consumer requests quickly and with minimal friction. Doing so requires gathering the right data from the consumer, using an efficient and minimally invasive approach.

Ultimately, organizations must employ the right level of friction at the right time as well as have an ability to execute CCPA compliance at scale. This saves on compliance costs and boosts operational efficiency.

Specifically, that means having access to an array of identity verification methods, including knowledge-based authentication, mobile one-time passwords, and mobile scan with escalation capabilities delivered securely in a manner that fosters customer engagement.

Requestors Are Not Required to Have or Set Up an Online Account

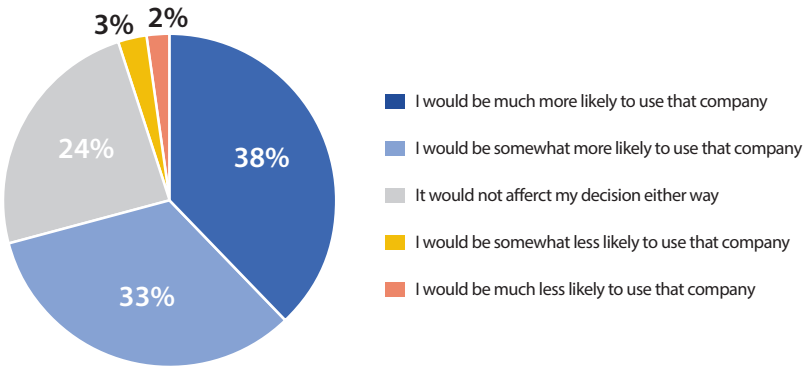
"A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information" (§ 1798.135(a)(1), prohibiting a business from requiring that a consumer create an account to exercise the consumer's right to opt out of the sale of personal information to third parties).

Top 5 things to do for CCPA IDV preparedness:

- Don't let CCPA identity verification become a new welcome door for fraudsters
- Remember that customers are not required to set up an online account
- Get familiar with the array of methods, channels, and use cases
- Understand that consumers have identity verification preferences
- Know how to integrate, scale, and automate

Consumers Prefer Companies that Demonstrate a Strong Commitment to their Identity Verification Processes

If you knew that a financial provider was using particularly more advanced identity verification methods, how would that affect your decision to choose that company?



N=1,499 US online consumers
Source: Second Annual Consumer Digital Identity Survey, IDology, 2019

And while some organizations may opt to verify identities using in-house personnel and processes, many others may opt for privacy platform providers with solutions that can be integrated seamlessly.

Nonetheless, under CCPA, the clock starts ticking once a consumer submits a request. Without automation in place, companies may resort to manual, time-consuming processes to prove an identity. They will also need to collect and store the personal information used to verify an identity in a secure manner. With a manual process, organizations run the risk of sharing data with an unverified user or worse, a cybercriminal.

Ad-hoc tools may also require extensive technical support and provide limited visibility into the workflow for inbound requests. This creates an inability to monitor individual requests or provide accurate updates to consumers regarding the status of their requests.

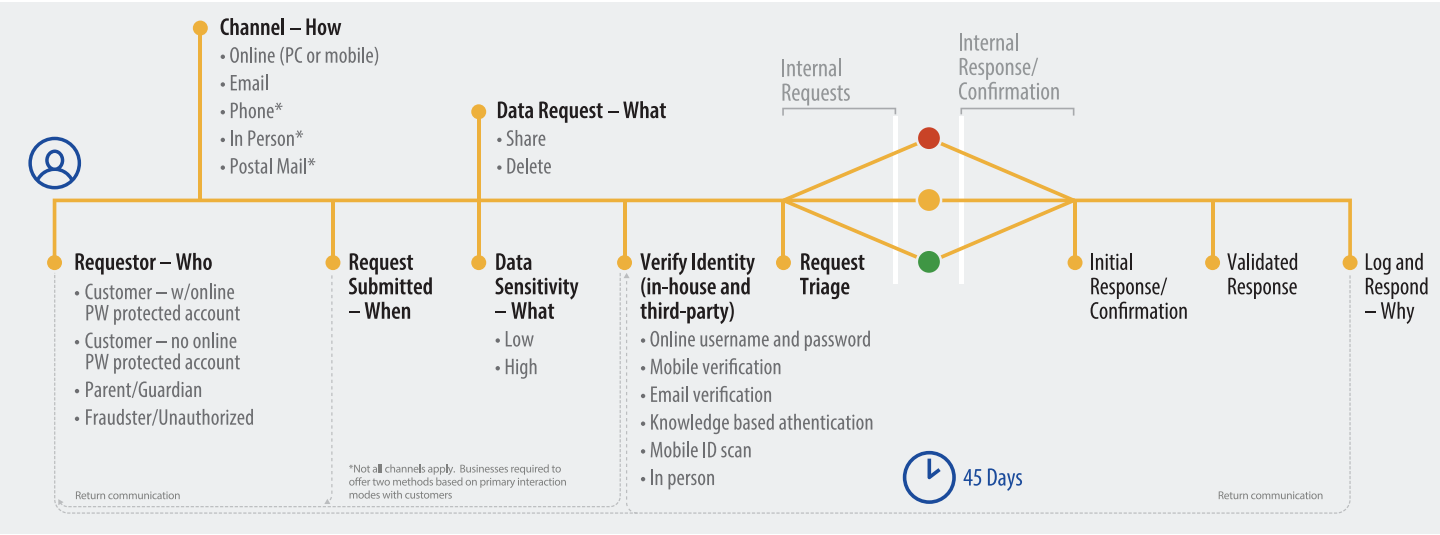
Upon receipt of a verifiable request, businesses must:

- Respond within 45 days
- Provide data from the last 12 months
- Provide data in a transferrable manner

"The the CCPA for the first time gives consumers a right to request specific information about how their personal data is processed, for what purposes, and with whom it is shared. The law also gives consumers the right to receive answers to these requests, free of charge, within 45 days, in an electronic format they can transfer to another business."

Source: iapp

Sample CCPA Report Workflow



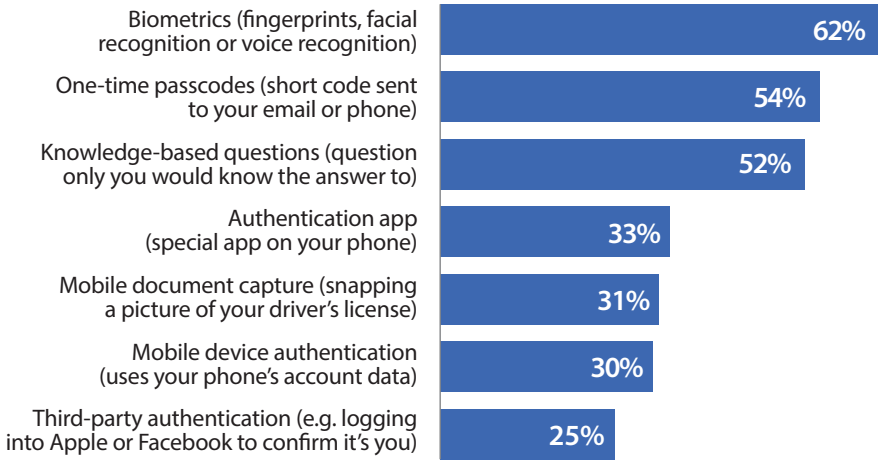
Source: Workflow based in part from "How to Prepare for the CCPA and Navigate Consumer Privacy Rights", Gartner, 2019

Consumers Need Options to Prove Their Identity

Given the diversity of today's consumers, organizations need access to a range of identity verification tools. Regardless of the user's chosen method, the goal remains the same: to fulfill the request quickly and accurately and only deliver sensitive data to the actual consumer. A broad range of IDV tools benefits both consumers and businesses.

Americans Utilize an Array of Identity Verification Methodologies with Differing Levels of Security Perceptions

There are methods available that can improve the security of your online accounts. How secure do you believe each of the following methods are?
Percent answering either "Extremely Secure" or "Very Secure."



Base: Combination of respondents who answered "Extremely Secure" or "Very Secure"
N = 1,499 US online consumers
Source: Second Annual Consumer Digital Identity Survey, IDology, 2019

Regardless of the technology at an organization's disposal, a convoluted process can alienate consumers. Similarly, a haphazard approach that shifts too much of the administrative burden to the consumer will not reflect well on the brand either. If the organization spends too much time verifying identities, there is even less time left to fulfill the request and satisfy customer service level commitments. An administratively burdensome approach also saddles the enterprise with excessive compliance-related costs and sends the wrong message to already anxious, impatient, or highly demanding consumers: that the enterprise has not allocated the appropriate resources to CCPA compliance.

While VCRs can place a considerable compliance burden on impacted companies, enlightened organizations can use them as a means of demonstrating their commitment to superior customer service. Just like the focus placed on optimizing other aspects of the customer's journey, VCRs deserve the same attention and investment. And while a flawless VCR process may not capture incremental revenue immediately, a less-than-optimal approach could contaminate the customer's perception of the brand and result in the loss of future revenue.

California Consumer Privacy Act (CCPA) Timeline and Enforcement

2018

March
– Cambridge Analytica

May
– CA data privacy measure ballot initiative collects 600K signatures

– GDPR in effect

June
– CCPA, officially ABA 375, signed into law

2019

March-May
– Public forums

May
– CA legislature considers amendments

October 10
– CA AG posts proposed regulations

2020

January 1
– CCPA goes into effect

July 1
– CA AG enforcement

CA. Attorney General Rule Making
CA AG establishing and issues rules and processes and regulations on Verifiable Consumer Requests for Identity Access

Conclusion

Progressive organizations should think about CCPA as an opportunity to engage with their customers, but it is imperative to get it right. With consumers being able to sue, the compliance risk is enormous. Some experts view CCPA as "the asbestos class-action suits of our time." That's why customer engagement during such a critical time matters. As companies become accustomed to CCPA, consumers will expect multiple IDV options that they can select quickly and use seamlessly.

Nonetheless, CCPA comes with a number of potential hurdles: individuals don't need an account to initiate a request, parents can make a request on behalf of minors, and fraudsters could exploit CCPA to get their hands on sensitive personal data. Compliance hinges on an organization's ability to embrace automation and deploy a scalable, secure approach to fulfilling VCRs.

With that said, there's too much at stake to be careless or cavalier about fulfilling VCRs. That's why it makes good business sense to work with identity verification experts with the ability to provide multiple methods to address multiple channels and an array of sensitivity conditions. This lets your customers know you take their privacy, data, and relationship with your company seriously.

In the CCPA IDV sphere, IDology's products are uniquely suited to offer a seamless transition to compliant, user-friendly identity authentication and verification. With IDology solutions, businesses can:

- Manage all data requestor types and channels via one flexible and easily deployed system
- Use multiple smart layers of identity attributes to locate and approve more legitimate customer requests with minimal friction
- Easily employ higher levels of authentication with integrated escalation methods
- Deter fraud with access to a consortium network of fraud intelligence, including network request velocity
- Track patterns and make informed decisions with advanced reporting and transparent reason notes

About IDology

IDology offers real-time and on-demand identity verification and fraud prevention solutions for organizations operating in the digital environment. The IDology platform serves as a collaborative hub for monitoring and stopping fraudulent activity while also driving revenue, decreasing costs, and meeting compliance requirements.

For details on how IDology can help your business onboard and verify customers, visit **www.idology.com**.

Visit **IDology.com /CCPA** for easy-to-deploy, best-in-class CCPA compliance and identity verification solutions.

IDOLOGY
a GBG company