

OFFICE OF LEGISLATIVE RESEARCH
PUBLIC ACT SUMMARY



PA 25-113—sSB-1295
General Law Committee

AN ACT CONCERNING BROADBAND INTERNET, GAMING, SOCIAL MEDIA, ONLINE SERVICES AND CONSUMER CONTRACTS.

TABLE OF CONTENTS:

[§§ 1 & 23 — NET EQUALITY PROGRAM](#)

Establishes a Net Equality Program by September 30, 2026, to allow eligible individuals to request to subscribe to affordable broadband Internet access

[§§ 2 & 24 — DELIVERY SERVICES FOR LOTTERY TICKETS](#)

Sets conditions for CLC to use an unlicensed delivery service to deliver lottery tickets

[§§ 2 & 24 — CLC LICENSED EMPLOYEES](#)

Allows CLC's licensed employees to receive endorsements on their licenses, rather than get a separate license, to work on different forms of gaming for CLC

[§§ 2 & 24 — VENDOR, AFFILIATE, LOTTERY SALE AGENT, AND CLC OCCUPATIONAL LICENSES](#)

Specifies cause for taking action against certain licensees and authorizes a summary suspension of a lottery sales agent's license for (1) keeping unauthorized gambling devices, illegitimate lottery tickets, and illegal bookmaking equipment or (2) allowing any illegal gambling at its retail facility

[§§ 3 & 24 — VOIDING SPORTS WAGERS](#)

Codifies rules on voiding and modifying wagers, which are substantially similar to those in existing regulations

[§§ 4, 13 & 25 — SOCIAL MEDIA PLATFORMS](#)

Requires social media platform owners, by October 1, 2026, to incorporate an online safety center and create a policy for handling reports of cyberbullying on the platform; prohibits social media platforms from requiring a minor's parent or legal guardian to create a social media account to submit such a request to unpublish a minor's account

[§§ 5-12, 18 & 25 — CONNECTICUT DATA PRIVACY ACT \(CTDPA\)](#)

Starting in July 2026, expands and revises various aspects of the Connecticut Data Privacy Act (CTDPA), such as (1) expanding who is generally covered under the act and modifying the list of exemptions, (2) expanding what data is considered "sensitive" and subject to additional protections, and (3) requiring impact assessments for those who do certain data profiling

[§§ 8, 9, 14-18 & 25 — MINORS AND ONLINE SERVICES, PRODUCTS, AND FEATURES](#)

OLR PUBLIC ACT SUMMARY

Starting in July 2026, revises various aspects of the CTDPA in relation to data processing for online services, products, and features for minors, such as (1) broadening what is considered heightened risk of harm to minors and (2) generally prohibiting certain practices by eliminating provisions allowing the minor or parents or guardian to consent to them

§§ 19 & 25— MOTOR VEHICLE DATA PRIVACY FOR SURVIVORS OF CERTAIN CRIMES

Creates a process by which an adult survivor of certain crimes (e.g., domestic violence) can submit a request to the motor vehicle manufacturer with a connected vehicle services account to take certain actions to prevent the abuser from remotely obtaining data from the vehicle

§§ 20 & 26 — AUTOMATIC RENEWAL AND CONTINUOUS SERVICE

Adds a provision on consideration of whether records of consent to renewal or continuous service comply with certain laws

§§ 21 & 26 — MOTOR VEHICLE QUOTED PRICES AND CERTAIN ADD-ON FEES

Requires fees, charges, and costs for add-on consumer goods or services to be included in the price and separately stated in the quoted price of a motor vehicle; prohibits advance printing of orders and forms with these fees, charges, and costs included

§ 22 — HOME IMPROVEMENT CONTRACTOR ADVERTISING

Allows certain home improvement contractors to satisfy the requirement that they include the fact of their registration and registration number in their advertisements by including in the advertisement a phone number or link to a website where a person can get or view a statement about the contractor's registration and the registration number

SUMMARY: This act makes various unrelated changes to broadband Internet access; state gaming laws and procedures, including for the lottery and sports wagering; social media platforms; the Connecticut Data Privacy Act (CTDPA), including in relation to data processing for online services, products, and features for minors; motor vehicle data privacy for survivors of certain crimes; automatic renewals and continuous service agreements; motor vehicle quoted prices; and home improvement contractor advertising.

EFFECTIVE DATE: various, as noted below.

§§ 1 & 23 — NET EQUALITY PROGRAM

Establishes a Net Equality Program by September 30, 2026, to allow eligible individuals to request to subscribe to affordable broadband Internet access

The act requires the Department of Energy and Environmental Protection (DEEP) commissioner to develop a Net Equality Program by September 30, 2026. As part of the program, a qualified broadband Internet access service provider must (1) allow eligible individuals to request to subscribe to affordable broadband Internet access service ("affordable broadband"), (2) make a commercially reasonable effort to raise public awareness of affordable broadband's availability, and (3) have enrollment procedures for affordable broadband on its website.

OLR PUBLIC ACT SUMMARY

The act generally limits the maximum monthly charge for affordable broadband to \$40 and requires certain minimum speeds to be 100 megabits per second (Mbps) download speed and five Mbps upload speed for the program's first year and then 20 Mbps upload speed afterwards.

Beginning January 31, 2027, the act requires state agencies proposing to contract for the purchase of broadband Internet access service, when all other factors are equal, to give preference to providers that offer affordable broadband to eligible households. The act states that it does not impair any contract that exists on October 1, 2026.

Regardless of any state law, the act specifies that no violations of the Net Equality Program provisions are deemed an unfair method of competition or an unfair or deceptive act or practice under the Connecticut Unfair Trade Practices Act (CUTPA, see BACKGROUND).

Program Requirements and Definitions

Beginning October 1, 2026, the act requires each qualified broadband Internet access service provider (i.e. a provider that does business in the state and with any state agency, other than the Department of Emergency Services and Public Protection (DESPP)), to allow individuals residing in eligible households in the provider's service territory to request to subscribe to the provider's affordable broadband service. Under the act, an "eligible household" is a household (1) with at least one resident enrolled in the supplemental nutrition assistance program (SNAP) or a public assistance program the provider uses to determine eligibility for its existing low-income Internet program and (2) located in the provider's service territory in the state.

A "broadband Internet access service provider" is an entity that provides broadband Internet access service through facilities occupying public highways or streets authorized by the Public Utilities Regulatory Authority, including through a certificate of public convenience and necessity, a certificate of video franchise authority, a certificate of cable franchise authority, or as a certified telecommunications provider.

The act also requires these providers, starting October 1, 2026, to make a commercially reasonable effort to raise public awareness about the availability of the affordable broadband service the provider offers to eligible households located in the provider's service territory. These efforts must include posting the enrollment procedures in a prominent and publicly accessible location on their website.

The act requires each service provider, starting by February 1, 2027, to annually submit to DEEP a report, as the commissioner sets, disclosing the number of eligible households that signed up for, and separately the number that received, its affordable broadband during the reporting year.

The act also requires DEEP, as part of the program, to explore options to establish and advance strategic and effective public-private partnerships.

Monthly Price

OLR PUBLIC ACT SUMMARY

The act generally caps a qualified broadband Internet access service provider's maximum monthly charge to an eligible household for affordable broadband service at \$40, including all taxes, charges, and fees, including for all equipment associated with the Internet access.

However, under the act, starting by June 1, 2027, DEEP must annually adjust the maximum monthly cost for the 12-month period starting the following July 1 based on any change in the consumer price index for the preceding calendar year, as published by the U.S. Department of Labor's Bureau of Labor Statistics.

Service Speeds

The act requires that all affordable broadband provided under its provisions have minimum speeds of:

1. 100 Mbps download speed and five Mbps upload speed between October 1, 2026, and September 30, 2027, and
2. 100 Mbps download speed and 20 Mbps upload speed after October 1, 2027.

In either case, the service speeds and latency must be sufficient to support distance learning and telehealth services.

Beginning June 1, 2030, and then not more frequently than biennially, the act allows DEEP, in consultation with its Bureau of Energy and Technology and the Department of Administrative Services' Commission for Educational Technology, to increase the affordable broadband plans' required minimum speeds for the two-year period beginning the following July 1. DEEP, the bureau, and the commission must post the increased speeds on their respective websites.

The act allows DEEP to approve or require a deviation from the service speed requirements to comply with applicable state or federal law or elements of DEEP's federally subsidized broadband programs that are included in federal applications that are made public or negotiated with bidders on or before June 30, 2025. However, it prohibits DEEP from approving any deviation that would provide affordable broadband service speeds that are slower than what the act requires or those established by DEEP, in consultation with the bureau and commission, whichever speeds are higher.

Conducting Business With State Agencies

Beginning January 31, 2027, the act requires state agencies proposing to contract for the purchase of broadband Internet access service, when all other factors are equal, to give preference to providers that offer affordable broadband to eligible households. Under the act, a "state agency" is any office; department, except DESPP; board; council; commission; institution; constituent unit of the state's higher education system; technical education and career school; or other executive, legislative, or judicial branch agency.

The act would have repealed a similar Net Equality Program provision in another bill, but that bill did not pass and the repeal has no legal effect (§ 23).

EFFECTIVE DATE: July 1, 2025 (the repeal of the provisions in another bill would

have been effective upon passage).

§§ 2 & 24 — DELIVERY SERVICES FOR LOTTERY TICKETS

Sets conditions for CLC to use an unlicensed delivery service to deliver lottery tickets

The act allows the Connecticut Lottery Corporation (CLC) to use a business that is not a licensed vendor as a delivery service to transport and deliver lottery tickets to lottery sales agents under certain circumstances.

To do so, CLC must give the Department of Consumer Protection (DCP) a detailed plan, in a form and way set by DCP, that includes:

1. the business's name and contact information,
2. the proposed date that the business will start shipping for CLC,
3. a detailed description of the tamper-evident packaging that will be used and its security features,
4. the business's security measures during delivery, and
5. the process used by the business if delivery is not successful.

DCP must review and either approve or deny the plan within 30 days after receiving it. CLC must keep copies of its plan documents for at least three years.

In order to use the delivery service:

1. CLC employees must securely package the tickets in tamper-evident packaging on CLC premises while under video surveillance;
2. the exterior packaging must not indicate that it contains lottery tickets and "lottery" cannot appear on the packaging, including in the return address;
3. the packages must be tracked and require a signature on delivery; and
4. CLC must document each package with its lottery game number and name, number of packs and pack numbers, lottery sales agent's name and address, package shipment date, and the name of the business delivering the tickets.

If a lottery sales agent tells CLC that a package of tickets is damaged, missing, or compromised, CLC must immediately tell DCP and give the agent instructions to embargo the package until its contents are verified by CLC's documentation.

Generally, under existing law, a person or business awarded a primary contract to provide facilities, components, goods, or services necessary for and directly related to CLC's secure operation of activities must receive a vendor license from DCP.

The act repeals identical provisions in PA 25-112, § 4.

EFFECTIVE DATE: October 1, 2025, except the repeal of provisions in PA 25-112 is effective upon passage.

§§ 2 & 24 — CLC LICENSED EMPLOYEES

Allows CLC's licensed employees to receive endorsements on their licenses, rather than get a separate license, to work on different forms of gaming for CLC

By law, CLC staff members must be licensed by DCP as class III and IV occupational licensees. Previously, staff members who worked on its "Internet games" (online lottery, online keno, or online sports wagering) or retail sports

OLR PUBLIC ACT SUMMARY

wagering needed to get additional licensing. The act allows CLC employees and job applicants to instead receive endorsements on their CLC license, rather than having to get a separate DCP license.

The act requires each applicant for a class III or IV license and each currently licensed CLC employee, as of January 1, 2026, to disclose in a DCP-prescribed way the types of gaming the applicant or licensed employee will work on at CLC. For these individuals, the DCP commissioner may issue a separate endorsement allowing them to operate CLC's Internet games or retail sports wagering. Under the act, these employees do not have to apply for a separate DCP gaming license.

The act requires these CLC staff members to report to DCP any criminal conviction within two business days after any conviction order or judgment. CLC and its employees must immediately report to DCP any change in an employee's scope of employment that would require the employee to get an additional endorsement.

The act repeals identical provisions in PA 25-112, § 4.

EFFECTIVE DATE: October 1, 2025, except the repeal of provisions in PA 25-112 is effective upon passage.

§§ 2 & 24 — VENDOR, AFFILIATE, LOTTERY SALE AGENT, AND CLC OCCUPATIONAL LICENSES

Specifies cause for taking action against certain licensees and authorizes a summary suspension of a lottery sales agent's license for (1) keeping unauthorized gambling devices, illegitimate lottery tickets, and illegal bookmaking equipment or (2) allowing any illegal gambling at its retail facility

The law allows DCP to reject a license application for, or suspend or revoke the license of, a vendor, affiliate, lottery sale agent, or CLC employee for good cause (see BACKGROUND). The law requires DCP to hold a hearing before revoking or suspending a license and the act also requires a hearing and cause before denying an application for, refusing to renew, or placing conditions on one of these licenses. DCP may also impose a civil penalty of up to \$2,500 for cause after a hearing (the act specifies that the \$2,500 civil penalty is for each violation).

The act specifies that cause for taking these actions includes:

1. failing to comply with the state's laws governing the lottery;
2. conduct likely to mislead, deceive, or defraud the public or DCP;
3. providing materially false or misleading information;
4. a criminal conviction or civil judgment involving fraud, theft, or financial crime;
5. insolvency, including filing for bankruptcy or failing to meet a material financial obligation that directly impacts the licensee's ability to comply with the laws governing the lottery; or
6. failing to complete an application.

The law allows DCP to require vendor and affiliate licensees to maintain books and records. The act adds that DCP can require these licensees to provide these books and records to DCP to ensure regulatory compliance.

The act repeals nearly identical provisions in PA 25-112, § 4.

Summary Suspension of Lottery Sales Agent's License for Certain Illegal Gambling Activities or Devices

The act prohibits lottery sales agents from (1) keeping unauthorized gambling devices, illegitimate lottery tickets, and illegal bookmaking equipment or (2) allowing any illegal gambling at its retail facility. DCP can fine an agent up to \$4,000 per violation.

DCP must issue the agent a notice of violation that includes an order that summarily suspends the agent's license and informs the agent:

1. about the fine imposed and the license's suspension,
2. to immediately cease activities that require a license, and
3. that the agent has 15 days after receiving the notice to request a hearing in writing.

If a hearing is not requested, the summary suspension and fine are final decisions that are appealable to court.

A summary suspension remains in effect until it is lifted and all fines are paid. It can be lifted by a written order of the DCP commissioner or based on a final decision after a hearing.

The act repeals identical provisions in PA 25-112, § 4.

EFFECTIVE DATE: October 1, 2025, except the repeal of provisions in PA 25-112 is effective upon passage.

§§ 3 & 24 — VOIDING SPORTS WAGERS

Codifies rules on voiding and modifying wagers, which are substantially similar to those in existing regulations

The act codifies rules on voiding and modifying wagers, which are substantially similar to those in existing regulations.

The act repeals similar provisions in PA 25-112, § 6.

Wagers That May Be Voided Without DCP Approval

The act permits an online gaming operator (see BACKGROUND) to void a sports wager without prior DCP approval if the wager is on:

1. a sporting event that was cancelled, delayed more than 24 hours from its original start time, or moved to a different venue;
2. sporting event players that do not take part in the event;
3. one or more acts in an event that does not occur;
4. a specific team qualifying for a post-season tournament and the number of teams allowed in the tournament has been reduced; or
5. an event and the format or number of players scheduled in a phase of the event has changed or the event is no longer scheduled to occur.

The operator must indicate the voided wager in the patron's account and promptly credit funds from a voided wager to the account.

The act requires a sports wagering retailer to post a notice telling patrons how

to know if a wager has been voided under the house rules (which the act defines as the terms and conditions for sports wagering) and how to get a refund. DCP must approve the form and manner of the notice, which must be at least 8.5" x 11" in size, have at least 20 point font, and be posted in a location where patrons place sports wagers.

Wagers That Must Be Modified or Voided Without DCP Approval

The act requires an operator to modify or void a sports wager without DCP approval if a patron requests it before the event that is the subject of the wager begins and:

1. the operator or its electronic wagering platform mistakenly communicated to the patron the wager's type, amount, or parameters or
2. a sports wagering retailer's employee made a mistake entering a wager in the platform.

Records

The act requires operators to maintain records of wagers that are voided or modified in a form and way set by DCP. The record for each wager must at least include:

1. the patron's name, unless the wager was placed at a retail sports wagering facility;
2. the reason for voiding or modifying the wager;
3. the type of wager, broken down by market;
4. the event associated with the wager and its date or dates; and
5. other information DCP requires to identify and assess the impact of voiding or modifying the wager.

Requests to DCP to Void Wagers

The act allows an operator to ask DCP in writing to void any wagers not covered above. DCP must establish the form and way of submitting these requests, which must at least include the:

1. reason for the request;
2. names of affected patrons, unless the wager was placed at a retail sports wagering facility;
3. event associated with the wager and its date or dates;
4. wager type;
5. total amount of the wager; and
6. plan to contact affected patrons, unless the wager was placed at a retail sports wagering facility.

After receiving a request, DCP can ask for additional information that it needs to review and assess the impact that granting the request will have on affected patrons and the integrity of gaming. The operator must provide this information.

An operator cannot void these wagers until it receives written approval from

DCP, in a form and way set by DCP.

Internal Controls

The act requires operators, by September 1, 2025, to give DCP, in a form and way set by DCP, their internal controls on voiding sports wagers and allocating patron funds. Under the act, “internal controls” are a master wagering licensee’s or online gaming operator’s written administrative and accounting procedures that ensure compliance with gaming laws, including financial reporting, operations’ effectiveness and security, “know your customer,” and fraud and money laundering deterrence.

DCP must ensure the internal controls:

1. give affected patrons notice within 24 hours after DCP approves a void request,
2. require prompt return of patron funds after voiding wagers, and
3. address any matter DCP believes is necessary to preserve gaming’s integrity.

By December 1, 2025, DCP must notify each operator whether it approves or disapproves of the controls. If approved, the operator must include the controls in its house rules and clearly and conspicuously on its platform.

EFFECTIVE DATE: July 1, 2025, except the repeal of provisions in PA 25-112 is effective upon passage.

§§ 4, 13 & 25 — SOCIAL MEDIA PLATFORMS

Requires social media platform owners, by October 1, 2026, to incorporate an online safety center and create a policy for handling reports of cyberbullying on the platform; prohibits social media platforms from requiring a minor’s parent or legal guardian to create a social media account to submit such a request to unpublish a minor’s account

Online Safety Center

The act requires each social media platform owner, by October 1, 2026, to incorporate an online safety center into the platform. An online safety center must at least give consumers who live in Connecticut and use the platform the following:

1. resources to (a) prevent cyberbullying on the platform and (b) enable them to identify ways to get mental health services, including a website address or telephone number to get services to treat an anxiety disorder or for suicide prevention services;
2. access to online behavioral health educational resources;
3. an explanation of the platform’s mechanism for reporting harmful or unwanted behavior, including cyberbullying on the platform; and
4. educational information about social media platforms’ impact on users’ mental health.

Under existing law and the act, a “social media platform” is a public or semi-public Internet service or application used by a Connecticut consumer that:

1. is primarily intended to connect and allow users to socially interact within

- the service or application and
2. enables a user to (a) construct a public or semi-public profile to sign into and use the service or application; (b) populate a public list of other users with whom the user shares a social connection within the service or application; and (c) create or post content seen by other users, including on message boards, in chat rooms, or through a landing page or main feed that also presents content from other users.

It is not a public or semi-public Internet service or application that:

1. only provides e-mail or direct messaging;
2. primarily has news, sports, entertainment, interactive video games, electronic commerce, or content the provider preselects or for which any chat, comments, or interactive functionality is incidental or directly related to, or dependent on, providing the content; or
3. is used by and under an educational entity's direction, including a learning management system or student engagement program.

Cyberbullying Policy

The act similarly requires each social media platform owner, by October 1, 2026, to establish a cyberbullying policy with a process for the owner to handle reports of cyberbullying on the platform.

Cyberbullying

For these provisions, “cyberbullying” is any act that (1) is reasonably likely to cause physical or emotional harm to a consumer or place him or her in fear of physical or emotional harm or (2) infringes on a consumer's rights under state or federal law.

Prohibition on Requiring Social Media Account for Request

Existing law requires social media platforms to unpublish a minor's social media account within 15 business days, and generally delete the account within 45 business days, after receiving an authenticated request. The act prohibits the platforms from requiring a minor's parent or legal guardian to create a social media account to submit such a request. But the platform may require the parent or legal guardian to use an existing account to submit the request, as long as the parent or legal guardian has access to the existing account.

The act would have repealed similar provisions on social media platforms in another bill, but that bill did not pass and the repeal has no legal effect (§ 25).
EFFECTIVE DATE: July 1, 2026 (the repeal of the provisions in another bill would have been effective upon passage)

§§ 5-12, 18 & 25 — CONNECTICUT DATA PRIVACY ACT (CTDPA)

Starting in July 2026, expands and revises various aspects of the Connecticut Data Privacy Act (CTDPA), such as (1) expanding who is generally covered under the act and modifying the list of

OLR PUBLIC ACT SUMMARY

exemptions, (2) expanding what data is considered “sensitive” and subject to additional protections, and (3) requiring impact assessments for those who do certain data profiling

Expansion of Applicability

The act generally expands the individuals and entities covered by the CTDPA’s requirements by lowering certain thresholds and adding additional categories.

Under prior law, the CTDPA applied to individuals and entities that did business in Connecticut or produced products or services targeting Connecticut residents and, during the preceding calendar year, controlled or processed personal data of at least:

1. 100,000 consumers, excluding personal data controlled or processed solely for completing a payment transaction, or
2. 25,000 consumers, and derived more than 25% of their gross revenue from selling personal data.

The act lowers the first threshold to 35,000 consumers and eliminates the second category above. It also extends the CTDPA (without any threshold) to apply to persons that (1) control or process consumers’ sensitive data (see below), excluding personal data controlled or processed solely for completing a payment transaction, or (2) offer consumers’ personal data for sale in trade or commerce.

Sensitive Data

Existing law prohibits controllers from processing sensitive data about a consumer (1) without consent, or (2) if the consumer is known to be a child under age 13, without following the Children’s Online Privacy Protection Act (COPPA) (15 U.S.C. § 6501 et seq.). Controllers must also conduct and document a data protection assessment for each of their processing activities that presents a heightened risk of harm to consumers (see below), including the processing of sensitive data. Under existing law, a “controller” is an individual or legal entity who, alone or jointly with others, determines the purpose and means of processing personal data.

The act additionally prohibits a controller from selling a consumer’s sensitive data without the consumer’s consent.

Under prior law, “sensitive data” was personal data that includes, among other things, (1) data revealing a mental or physical health condition or diagnosis, (2) the processing of genetic or biometric data used to uniquely identify an individual, and (3) personal data collected from someone known to be a child. (Under existing law, biometric data is data generated by automatic measurements of an individual’s biological characteristics and used to identify a specific individual.)

The act also expands the “sensitive data” covered by the law by:

1. including data revealing (a) a mental or physical disability or treatment or (b) nonbinary or transgender status;
2. specifying that it includes genetic or biometric data or information derived from the data, rather than only the processing of this data used to uniquely identify an individual; and
3. including personal data collected from an individual who the controller

willfully disregards is a child, rather than only when the controller has actual knowledge as under prior law.

The following are also considered sensitive data under the act:

1. neural data (any information generated by measuring an individual's central nervous system activity);
2. a consumer's financial account number or log-in information or credit or debit card numbers that, in combination with any required access or security code, password, or credential, would allow access to the account; or
3. government-issued identification number, such as Social Security, passport, state identification card, or driver's license numbers, that applicable law does not require to be publicly displayed.

Profiling

Under existing law, "profiling" is any form of automated processing done on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Opt-out, Review, and Related Rights. The act expands a consumer's right to opt out of personal data processing when the data is used for profiling to advance any, rather than only, automated decisions that produce legal or similarly significant effects concerning the consumer (see below). Additionally, if the consumer's personal data was processed for profiling purposes to further such an automated decision, the act gives the consumer, if feasible, the right to:

1. question the result of the profiling;
2. be informed of why the profiling resulted in the decision;
3. review his or her personal data processed for the profiling; and
4. if the profiling decision concerns housing, correct any incorrect personal data processed for profiling and have the profiling decision reevaluated based on the corrected data, taking into account the nature of the data and why it was processed.

As under existing law for other consumer requests, if a controller, using commercially reasonable efforts, cannot authenticate a consumer's request, the controller is not required to comply with the request to initiate an action under this provision. The controller must notify the consumer that it is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the consumer and his or her request.

Decision That Produces Any Legal or Similarly Significant Effect. Under prior law, "decisions that produce legal or similarly significant effects concerning a consumer" were controllers' decisions that resulted in providing or denying financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services. The act modifies the definition by (1) expanding it to also include any decision made on the controller's behalf that has this effect and (2) narrowing it by eliminating decisions that result in providing or denying access to essential goods or services.

Impact Assessments. Under the act, each controller that engages in any profiling for making a decision that produces a legal or similarly significant effect related to a consumer must conduct an impact assessment for the profiling. This assessment must include the following, to the extent reasonably known by or available to the controller, as applicable:

1. a statement by the controller disclosing the profiling’s purpose, intended use cases and deployment context, and benefits;
2. an analysis of whether the profiling poses any known or reasonably foreseeable heightened risk of harm to a consumer (see below), and if so, the (a) nature of the risk and (b) mitigation steps the controller has taken;
3. a description of the (a) main categories of personal data processed as inputs for the profiling and (b) outputs the profiling produces;
4. an overview of the main categories of personal data the controller used to customize the profiling, if applicable;
5. any metrics used to evaluate the profiling performance and known limitations;
6. a description of any transparency measures taken for the profiling, including any taken to disclose to consumers that the controller is engaged in the profiling while so engaged; and
7. a description of the post-deployment monitoring and user safeguards provided for the profiling, including the oversight, use, and learning processes the controller established to address issues arising from the profiling.

The act applies to these impact assessments the existing law’s provisions for data protection assessments, such as allowing (1) the attorney general to require certain disclosures, (2) a single assessment to address comparable operations with similar activities, and (3) compliance with another applicable law or regulation to satisfy the CTDPA requirements.

Under the act, these impact assessment requirements apply to processing activities created or generated on or after August 1, 2026, and are not retroactive.

Existing law requires processors to assist controllers by giving them information needed to conduct and document data protection assessments. The act also requires this assistance for impact assessments.

Under existing law, “heightened risk of harm to a consumer” generally includes (1) processing personal data for targeted advertising; (2) selling personal data; (3) processing personal data for profiling, where the profiling presents a reasonably foreseeable risk of certain outcomes; or (4) processing sensitive data.

Ability to Collect, Use, or Retain Data. The act specifies that the obligations it imposes on controllers, processors, or consumer health data controllers (and obligations on controllers or processors relating to online services, products, or features for minors; see below) do not restrict their ability to collect, use, or retain data for internal use to process personal data for profiling to further any automated decision that may produce any legal or similarly significant effect concerning a consumer, if the personal data is:

1. processed only to the extent needed to detect or correct any bias that may result from processing the data for profiling, the bias cannot effectively be

- detected or corrected without processing the data, and the data is deleted once the processing has been completed;
2. processed subject to appropriate safeguards to protect consumers' rights under the U.S. or state constitutions or laws;
 3. subject to technical restrictions on the reuse of the data and industry-standard security and privacy measures, including pseudonymization;
 4. subject to measures to ensure that the data is secure, protected, and subject to suitable safeguards, including strict data access controls and related documentation, to avoid misuse and limit data access to authorized individuals only while preserving the data's confidentiality; and
 5. not sent or transferred to, or otherwise accessed by, any third party.

The act also allows controllers, processors, or consumer health data controllers to collect, use, or retain data for internal operations, consistent with COPPA's internal operations exception, when processing data under that exception.

Publicly Available Information

Under existing law, publicly available information is not "personal data" and is not subject to the CTDPA.

Under prior law, "publicly available information" was information that (1) was lawfully available through federal, state, or municipal government records or widely distributed media and (2) a controller had a reasonable basis to believe the consumer had lawfully made available to the general public.

Under the act, information is considered publicly available if either one of these prior requirements is satisfied, rather than both. Simultaneously, for widely distributed media information, the act only requires that the controller have a reasonable basis to believe that the information has been lawfully made available to the general public.

The act specifies that any biometric data that can be associated with a specific consumer and was collected without the consumer's consent is not considered publicly available information.

Consumer Health Data

The CTDPA sets standards on accessing and sharing consumer health data and places various specific limitations on consumer health data controllers. The act expands what is considered "consumer health data" by including personal data that a controller uses to identify a consumer's physical or mental health status, not just a physical or mental health condition or diagnosis as under prior law.

Exemptions

The act revises provisions on which financial institutions are exempt from the CTDPA requirements. It removes financial institutions subject to the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) from prior law's list of exempted entities. But it exempts certain banks, credit unions, or their affiliates or

subsidiaries that (1) are only and directly engaged in financial activities as described in federal banking law, (2) are regulated and examined by the Banking Department or an applicable federal banking regulatory agency, and (3) have established a program to comply with applicable federal or state personal data-related requirements.

The act also exempts the following from the CTDPA:

1. candidate committees, national committees, party committees, or political committees;
2. insurers or their affiliates, fraternal benefit societies, health carriers, insurance-support organizations, insurance agents, or insurance producers; and
3. agents, broker-dealers, investment advisers, or investment adviser agents regulated by the state banking department or the federal Securities and Exchange Commission.

The act also exempts HIPAA covered entities' limited data sets (i.e. protected health information that excludes specific identifiers) that are used, disclosed, and maintained for research, public health, or health care operations (45 C.F.R. § 164.514(e)).

Consumer Rights

Under existing law, a consumer has the right to confirm whether or not a controller is processing the consumer's personal data and access the data. The act specifies that this includes any inferences about the consumer that are derived from the data and whether a controller or processor is processing the data for profiling to make a decision that produces a legal or similarly significant effect on a consumer (as defined above). As under existing law, this right is available unless the confirmation or access would require the controller to reveal a trade secret. The act also expands the exception to include when a controller is prohibited from disclosing certain personal information under the act (see below).

As under existing law for other requests, if a controller, using commercially reasonable efforts, cannot authenticate a consumer's request, the controller is not required to comply with the request to initiate an action under this provision. The controller must notify the consumer that it is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the consumer and his or her request.

Under the act, a controller cannot disclose certain personal data in response to a consumer's request to confirm whether data is being processed and to access the data. The controller must instead inform the consumer or person acting on his or her behalf, with sufficient particularity, that the controller has collected the personal data on the consumer's (1) Social Security number; (2) driver's license, state identification card, or other government-issued identification numbers; (3) financial account number; (4) health insurance or medical identification numbers; (5) account password; (6) security question or its answer; or (7) biometric data.

The act also gives a consumer the right to obtain from the controller (1) a list of the third parties to whom the controller has sold the consumer's personal data or

(2) if the controller does not maintain such a list, a list of all third parties to whom the controller has sold personal data; however, the controller does not have to reveal any trade secret.

Other Controller Requirements and Restrictions

Under prior law, a controller had to limit the collection of personal data to what was adequate, relevant, and reasonably necessary for data processing, as disclosed to the consumer. The act instead limits the data collection to what is reasonably necessary and proportionate to the disclosed purpose for processing the data.

Prior law generally prohibited controllers from processing personal data for purposes that were neither reasonably necessary to, nor compatible with, the purposes disclosed to the consumer, except with the consumer's consent. The act limits this provision to when the controller is processing personal data for any material new purpose, and requires the controller to consider the consumer's reasonable expectation regarding the personal data at the time it was collected based on the disclosed purposes. The controller must also consider the following:

1. the relationship between the new purpose and the purposes that were disclosed to the consumer;
2. the impact that processing the data for the new purpose might have on the consumer;
3. the relationship between the consumer and the controller and the context in which the data was collected; and
4. whether there are any additional safeguards, such as encryption or pseudonymization, in processing the data for the new purpose.

Prior law prohibited controllers from processing sensitive data (see above) without consumer consent or, in the case of children, not in accordance with COPPA. The act further limits controllers from doing so unless it is reasonably necessary in relation to the purposes for which the sensitive data is processed.

Existing law prohibits controllers from processing personal data in violation of state laws that prohibit unlawful discrimination against consumers. The act specifies that any evidence, or lack of evidence, on proactive anti-bias testing or similar efforts to avoid processing the data in violation of the law are relevant to any claim available for a violation and any defense. This includes evidence (or the lack of evidence) on the quality, efficacy, recency, and scope of the test or effort; the results of the test or effort; and the response to these results.

Privacy Notice and Disclosure

Existing law requires controllers to give consumers a reasonably accessible, clear, and meaningful privacy notice. The act modifies the required notice in various ways as described below.

Notice on Third Parties and Targeted Advertising. Prior law required the notice to include the categories of personal data the controller shared with third parties and the categories of third parties with whom the controller shared personal data. Under the act, this pertains to data the controller sells instead of what is shared as

under prior law.

Under prior law, if a controller sold personal data to third parties or processed personal data for targeted advertising, the controller had to clearly and conspicuously disclose the processing. The act requires this disclosure to be included in the privacy notice.

Additional Privacy Notice Content. The act also requires the controller to include in the notice (1) disclosure of whether the controller collects, uses, or sells personal data to train large language models and (2) the most recent month and year during which the controller updated the privacy notice.

Under the act, a controller must make the required privacy notice publicly available:

1. through a conspicuous hyperlink that includes the word “privacy” (a) on the homepage of the controller’s website, if the controller maintains one; (b) on a mobile device’s application store page or download page, if maintained by the controller; and (c) on the application’s settings menu or in a similarly conspicuous and accessible location, if the controller maintains an application for use on a mobile device or other device used to connect to the Internet;
2. through a medium where the controller regularly interacts with consumers, including mail, if the controller does not maintain a website;
3. in each language in which the controller (a) provides any product or service that is subject to the privacy notice, or (b) carries out any activity related to such a product or service; and
4. in a way that is reasonably accessible to, and usable by, individuals with disabilities.

Notice of Retroactive Material Change. Whenever a controller makes any retroactive material change to the privacy notice or practices, the act requires the controller to (1) notify affected consumers about any personal data to be collected after the change’s effective date and (2) give them a reasonable opportunity to withdraw consent to any further and materially different collection, processing, or transfer of previously collected personal data after the material change.

The controller must also take all reasonable electronic measures to give the notice to affected consumers, considering the available technology and the nature of the controller’s relationship with these consumers.

Connecticut-Specific Notice Not Required. The act specifies that it does not require a controller to have a privacy notice that is specific to Connecticut if the controller has a generally applicable privacy notice that satisfies the established requirements.

Processors’ Assistance to Controllers

Under existing law, a processor must assist the controller in meeting the controller’s obligations under the CTDPA. Under prior law, this had to include, while considering the nature of processing and the information available to the processor by appropriate technical and organizational measures, as reasonably practicable, help fulfilling the controller’s obligation to respond to a request from a

consumer exercising his or her rights under the CTDPA.

The act eliminates the requirement that processors consider the appropriate technical and organizational measures and available information, and requires them to assist in responding to these consumer requests if possible, rather than when it is reasonably practicable.

The act would have repealed similar CTDPA provisions in another bill, but that bill did not pass and the repeal has no legal effect (§ 25).

EFFECTIVE DATE: July 1, 2026, (the repeal of the provisions in another bill would have been effective upon passage)

§§ 8, 9, 14-18 & 25 — MINORS AND ONLINE SERVICES, PRODUCTS, AND FEATURES

Starting in July 2026, revises various aspects of the CTDPA in relation to data processing for online services, products, and features for minors, such as (1) broadening what is considered heightened risk of harm to minors and (2) generally prohibiting certain practices by eliminating provisions allowing the minor or parents or guardian to consent to them

The CTDPA also establishes a framework and sets requirements for how individuals or entities offering certain online services, products, and features manage and process personal data for minors (i.e. those under age 18).

Heightened Risk of Harm to Minors

Existing law requires a controller with consumers who are minors to use reasonable care to avoid causing any heightened risk of harm to minors in processing their personal data. The act broadens what constitutes “heightened risk of harm to minors” by also including the reasonably foreseeable risk of the following:

1. any physical violence against minors;
2. any material harassment of minors on any online service, product, or feature, where it is severe, pervasive, or objectively offensive to a reasonable person; or
3. any sexual abuse or sexual exploitation of minors.

Under prior law, heightened risk of harm to minors included the reasonably foreseeable risk of any (1) financial, physical, or reputational injury to minors or (2) physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of minors if the intrusion would be offensive to a reasonable person. Under the act, the injury or intrusion must be material. As under existing law, the heightened risk also includes unfair or deceptive treatment of, or any unlawful disparate impact on, minors.

In broadening the definition, the act expands the circumstances when controllers must do data protection assessments to include these new risk factors and make and implement plans to mitigate or eliminate the risk. By law, each controller with consumers who are minors must (1) do a data protection assessment of its online service, product, or feature to address any heightened risk of harm to minors that is a reasonably foreseeable result of offering the online service, product,

or feature to minors and (2) when applicable, make and implement a plan to mitigate or eliminate the risk.

By law, an “online service, product, or feature” is any service, product, or feature provided online, but not (1) telecommunications or broadband Internet access service or (2) delivery or use of a physical product.

Willfully Disregard That Consumer is a Child

Under prior law, certain CTDPA requirements specifically required actual knowledge that a consumer was a child as defined in COPPA (i.e. under age 13). The act expands this to include instances where the controller willfully disregards that the consumer is a child. The additional standard applies to provisions (1) allowing a parent or legal guardian to exercise consumer rights on a child’s behalf for a controller’s personal data processing and (2) prohibiting controllers from processing sensitive data concerning a child except in accordance with COPPA.

Processing Data for Targeted Advertising of Certain Minors

Prior law prohibited controllers from processing a consumer’s personal data for targeted advertising or selling the data without the consumer’s consent, for consumers ages 13 to 15. The act eliminates a minor’s ability to consent and expands the age threshold to include 16- and 17-year-olds.

Certain Other Consent Provisions Eliminated

Under prior law, controllers that offered an online service, product, or feature to minors could take certain actions if they received the minor’s consent or, if the minor was younger than age 13, the minor’s parent’s or legal guardian’s consent. The act eliminates the ability for someone to consent for certain provisions, thus generally prohibiting them.

Specifically, under the act, these controllers are now generally prohibited from:

1. processing a minor’s personal data for targeted advertising and personal data sales or collecting the minor’s precise geolocation (see below);
2. using a system design feature to significantly increase, sustain, or extend a minor’s use of the online service, product, or feature; or
3. processing a minor’s personal data unless it is (a) reasonably necessary to provide the online service, product, or feature and (b) for the disclosed purpose.

As under prior law, these provisions do not apply to an educational entity’s services or applications, including a learning management system or a student engagement program.

Precise Geolocation

The act further limits when a controller that offers an online service, product, or feature to minors may collect a minor’s precise geolocation data to circumstances

when it is strictly, rather than reasonably, necessary for the controller to provide the online service, product, or feature. Existing law additionally requires a controller, when collecting this data, to give the minor a signal indicating that the collection is occurring.

Automated Decisions

The act prohibits controllers that offer any online service, product, or feature to a minor from profiling to advance any automated decisions that produce legal or similarly significant effects concerning the minor (e.g., concerning education enrollment or health care services), subject to applicable consent requirements. Prior law limited this to apply only when the decision being advanced is fully automated.

Unsolicited Communications to Minors

The act prohibits a controller from offering direct messaging for use by minors unless it has readily accessible and easy-to-use safeguards to allow a minor or a minor's parent or legal guardian to prevent adults that the minor is not connected with from sending unsolicited communications to the minor. It also requires this safeguard to be the default setting. Under prior law, controllers only needed to have readily accessible and easy-to-use safeguards to limit an adult's ability to send these unsolicited communications.

As under existing law, these provisions do not apply to (1) email or (2) direct messages that are shared between the sender and recipient and not posted publicly or visible by anyone else.

Impact Assessment

Similar to the impact assessment requirements for controllers generally (see above), the act requires an impact assessment for any controller that offers any online service, product, or feature to a minor if it does any profiling based on the consumer's personal data. The controller must do these assessments if it has actual knowledge, or willfully disregards, that the consumer is a minor. It requires a processor to provide any information needed for a controller to conduct and document an impact assessment. As under existing law, processors must adhere to a controller's instructions and assist the controller in meeting its obligations under the CTDPA.

Required Components. The impact assessment must include, to the extent reasonably known by or available to the controller, similar information as for impact assessments by controllers generally (see above). Among other differences, for online services for minors, the act does not require the assessment to include metrics used to evaluate the profiling's performance and known limitations.

The act extends to these impact assessments various provisions that existing law applies to data protection assessments, such as:

1. requiring controllers to review the assessment as needed to account for

- material changes to certain operations,
- 2. allowing a single assessment to address comparable operations with similar activities,
- 3. allowing compliance with another applicable law or regulation to satisfy the CTDPA requirements, and
- 4. a rebuttable presumption that a controller used reasonable care if it complied with the impact assessment requirements.

Plan to Mitigate or Eliminate Risk. As under existing law for data protection assessments, if an impact assessment shows that the online service, product, or feature poses a heightened risk to minors, the controller must make and implement a plan to mitigate or eliminate the risk.

For both types of assessments, the act also allows the attorney general to require a controller to disclose to him a plan to mitigate or eliminate the risk, if the plan is relevant to an attorney general investigation. The controller must disclose the plan within 90 days after the attorney general notifies the controller about the required disclosure.

Exempt From Disclosure. As is the case under existing law for data protection assessments, under the act, impact assessments and harm mitigation or elimination plans (for either type of assessment) are confidential and exempt from disclosure under the Freedom of Information Act. If any information in an assessment or plan is disclosed to the attorney general and subject to the attorney-client privilege or work product protection, the disclosure does not waive the privilege or protection.

Internal Operations

The CTDPA specifies that the obligations it imposes on controllers or processors who offer online services, products, or features to minors do not restrict their ability to collect, use, or retain data for internal use to, among other things, perform internal operations such as those that are reasonably aligned with the consumer's expectations. The act narrows the internal operation performances under these provisions to instances where the controllers and processors perform solely internal operations.

The act would have repealed similar CTDPA provisions related to minors in another bill, but that bill did not pass and the repeal has no legal effect (§ 25).

EFFECTIVE DATE: July 1, 2026, (the repeal of the provisions in another bill would have been effective upon passage).

§§ 19 & 25— MOTOR VEHICLE DATA PRIVACY FOR SURVIVORS OF CERTAIN CRIMES

Creates a process by which an adult survivor of certain crimes (e.g., domestic violence) can submit a request to the motor vehicle manufacturer with a connected vehicle services account to take certain actions to prevent the abuser from remotely obtaining data from the vehicle

The act allows survivors of certain crimes (e.g., domestic violence) to submit a connected vehicle service request to a covered provider (i.e. motor vehicle manufacturer, or entity acting on its behalf, that provides a connected vehicle

service) to take certain actions to prevent an abuser (see definition below) from remotely obtaining data from, or sending commands to, a vehicle.

Definitions

Under the act, a “survivor” is an adult (age 18 or older) against whom a covered act was committed or allegedly committed.

A “covered act” is an action that is a:

1. crime under the federal Violence Against Women Act of 1994, such as domestic violence, dating violence, economic abuse, and stalking (34 U.S.C. § 12291(a));
2. severe form of trafficking in persons or sex trafficking under federal law (22 U.S.C. § 7102 (11) & (12)); or
3. crime, act, or practice that is (a) similar to those described above and (b) prohibited under federal, state, or tribal law.

A “connected vehicle service request” is a survivor’s request to terminate or disable the abuser’s access to a connected vehicle service.

An “abuser” is an individual who (1) a survivor identifies in a connected vehicle service request and (2) has committed, or allegedly committed, a covered act against the survivor who made the service request.

A “connected vehicle service” is any capability a motor vehicle manufacturer provides that allows a person to remotely obtain data from, or send commands to, a covered vehicle, including through a mobile device software application.

A “covered vehicle” is one that is (1) the subject of a connected vehicle request and (2) identified by a survivor under the act’s provisions.

Survivor’s Connected Vehicle Service Request

Under the act, survivors requesting that a connected vehicle service be terminated or disabled must include the vehicle identification number (VIN), the abuser’s name, and certain proof of ownership or possession of the vehicle. Proof of ownership or possession must include at least the following, as applicable:

1. proof that the survivor is the vehicle’s sole owner;
2. if the survivor is not the sole owner, proof that the survivor is legally entitled to exclusively possess the vehicle, such as a court order awarding exclusive possession to the survivor; or
3. if the abuser owns the vehicle in whole or in part, a dissolution of marriage decree, restraining order, or temporary restraining order that names the abuser and (a) gives the survivor exclusive possession of the vehicle or (b) restricts the use of a vehicle service by the abuser against the survivor.

Covered Provider Required Actions

Within two business days after a survivor submits a connected vehicle service request, the covered provider must take one or more of the following actions, whether or not the abuser is an account holder:

OLR PUBLIC ACT SUMMARY

1. terminate or disable the covered connected vehicle services account associated with the abuser;
2. terminate or disable the covered connected vehicle services or services account associated with the covered vehicle, including by resetting or deleting its data or wireless connection, and giving the survivor instructions to reestablish the services or account; or
3. if the motor vehicle has an in-vehicle interface, informing the survivor about the interface's availability and how to use it to terminate or disable the connected vehicle services.

Denial of Abuser Request

After the covered provider has acted, the provider must deny any request the abuser makes to obtain data (1) generated by the connected vehicle service after the abuser's access to the service was terminated or disabled due to the survivor's request and (2) that the covered provider maintains.

Covered Provider's Requirement to Act

Other than for a service request lacking the required information, the act prohibits a covered provider from refusing to take the actions listed above based on other requirements not being satisfied, including any requirement for:

1. paying any fee, penalty, or other charge;
2. maintaining or extending the term of the covered connected vehicle services account;
3. obtaining approval from any account holder other than the survivor; or
4. increasing the rate charged for the connected vehicle service.

Notice to Survivor Required Before Notifying Abuser

If the covered provider intends to give the abuser any formal notice about any of the actions above, the provider must first notify the survivor about when it intends to do so.

The act requires the covered provider to take reasonable steps to ensure that it only gives the abuser formal notice (1) at least three days after the provider notified the survivor and (2) after the provider has terminated or disabled the abuser's access to the connected vehicle service.

When Action is Not Operationally or Technically Feasible

Under the act, covered providers are not required to take any of the actions above if the provider cannot operationally or technically perform them. If that is the case, the provider must promptly notify the survivor who submitted the request. The notice must at least disclose whether the covered provider's inability to perform the action operationally or technically can be remedied and any steps the survivor can take to assist the provider in doing so.

Confidentiality of Request-Related Information

The covered provider and its officers, directors, employees, vendors, or agents must treat all information the survivor submits as confidential and must securely dispose of the information within 90 days after the survivor's submission. The act prohibits a covered provider from disclosing connected vehicle service request-related information to a third party unless the (1) survivor affirmatively consents or (2) disclosure is necessary to perform the connected vehicle service request.

The act specifically allows covered providers to maintain records for longer than 90 days if they are reasonably necessary and proportionate to verify that the survivor fulfilled the conditions for a request.

Material Change Notifications

The survivor must take reasonable steps to notify the covered provider about any change in the ownership or possession of the covered vehicle that materially affects the need for the covered provider to take the required actions listed above.

Emergency Situations

Regardless of the requirements above, the act does not prohibit or prevent a covered provider from terminating or disabling an abuser's access to a connected vehicle service after receiving a service request in a situation that, if allowed to continue, poses an imminent risk of death or serious bodily harm.

Website Instructions

The act requires each covered provider to publicly post on its website a statement describing how a survivor may submit a connected vehicle service request to the provider.

Immunity

The act provides immunity from civil liability to each covered provider and its officers, directors, employees, vendors, and agents for any act or omission that was done in compliance with these provisions.

The act would have repealed a similar provision on motor vehicle data privacy in another bill, but that bill did not pass and the repeal has no legal effect (§ 25).
EFFECTIVE DATE: July 1, 2026 (the repeal of the provisions in another bill would have been effective upon passage)

§§ 20 & 26 — AUTOMATIC RENEWAL AND CONTINUOUS SERVICE

Adds a provision on consideration of whether records of consent to renewal or continuous service comply with certain laws

OLR PUBLIC ACT SUMMARY

The law prohibits a business that enters a consumer agreement with automatic renewal or continuous service from charging a credit or debit card or other account unless the consumer affirmatively consents to the renewal or continuous service. The act requires a court or agency to consider whether the business produced a record of consent that complied with the law on recording phone calls, including eavesdropping, when considering whether a business obtained the required consent.

The act repeals a substantially similar provision in PA 25-111, § 41.

EFFECTIVE DATE: October 1, 2025, except the repeal of the provisions in PA 25-111 is effective upon passage.

§§ 21 & 26 — MOTOR VEHICLE QUOTED PRICES AND CERTAIN ADD-ON FEES

Requires fees, charges, and costs for add-on consumer goods or services to be included in the price and separately stated in the quoted price of a motor vehicle; prohibits advance printing of orders and forms with these fees, charges, and costs included

The law requires a car dealer quoting a sale price to separately state the dealer conveyance fee. The act requires the quote to (1) include any fee, charge, or cost for an optional add-on consumer good or service and (2) separately state the amount of each of these fees, charges, and costs, and that they are optional.

The act prohibits printing the dealer's order and invoice forms with fees, charges, and costs for optional add-on consumer goods or services before a discussion with a prospective buyer.

The act also makes technical and conforming changes.

The act repeals substantially similar provisions in PA 25-111, § 43.

EFFECTIVE DATE: October 1, 2025, except the repeal of provisions in PA 25-111 is effective upon passage.

§ 22 — HOME IMPROVEMENT CONTRACTOR ADVERTISING

Allows certain home improvement contractors to satisfy the requirement that they include the fact of their registration and registration number in their advertisements by including in the advertisement a phone number or link to a website where a person can get or view a statement about the contractor's registration and the registration number

The act allows certain home improvement contractors to satisfy the requirement that they include the fact of their registration and registration number in their advertisements by including in the advertisement a phone number or link to a website where a person can get or view a statement about the contractor's registration and the registration number. This applies if the contractor (1) is a publicly traded business listed on a U.S. stock exchange, (2) spends at least 30% of its advertising expenses on advertising at audiences in at least five states, and (3) is not advertising directly to a consumer.

Under existing law, home improvement contractors must also show their registration when asked to do so by any interested party.

By law, a violation of these advertising provisions is a CUTPA violation.

EFFECTIVE DATE: October 1, 2025

BACKGROUND

CUTPA

By law, CUTPA prohibits businesses from engaging in unfair and deceptive acts or practices. It allows the DCP commissioner, under specified procedures, to issue regulations defining an unfair trade practice, investigate complaints, issue cease and desist orders, order restitution in cases involving less than \$10,000, impose civil penalties of up to \$5,000, enter into consent agreements, ask the attorney general to seek injunctive relief, and accept voluntary statements of compliance. It also allows individuals to sue. Courts may issue restraining orders; award actual and punitive damages, costs, and reasonable attorney's fees; and impose civil penalties of up to \$5,000 for willful violations and up to \$25,000 for a restraining order violation.

CLC Vendors, Affiliates, Lottery Sales Agents, and Occupational Licensees

By law, a person or business needs a vendor license to be awarded a primary contract to provide facilities, components, goods, or services necessary for and directly related to CLC's secure operation of activities.

By law, a person or business needs an affiliate license to (1) be a contractor or subcontractor that provides facilities, components, goods, or services necessary for and directly related to CLC's secure operation of activities, or (2) exercise control over a vendor.

By law, a person needs a lottery sales agent license to contract with CLC to sell lottery tickets or offer keno at a retail facility.

By law, CLC employees and officials and certain others related to vendor and affiliate licensees must get an occupational license.

Online Gaming Operator

By law, an "online gaming operator" is a person or business that operates an electronic wagering platform and contracts directly with a master wagering licensee to provide (1) one or more Internet games or (2) retail sports wagering.

Master Wagering Licensee

By law, a "master wagering licensee" is generally the Mashantucket Pequot or Mohegan tribes or CLC.

Related Acts

As noted above, this act repeals provisions of PA 25-112, §§ 4 and 6, and contains substantially similar provisions related to (1) delivery services for lottery tickets; (2) CLC licensed employees; (3) vendor, affiliate, lottery sales agent, and

OLR PUBLIC ACT SUMMARY

CLC occupational licenses; and (4) voiding sports wagers.

As noted above, this act repeals provisions of PA 25-111, §§ 41 and 43, and contains substantially similar provisions related to (1) consumer agreements with automatic renewal and continuous service provisions and (2) quoted prices for motor vehicles and certain add-on fees.

PA 25-44 requires businesses that enter into a consumer agreement that includes an automatic renewal or continuous services provision to (1) send consumers an annual reminder with certain information and (2) enable consumers to stop the renewal or services through a website, email, or telephone.