
DEPARTMENT OF COMMERCE

Division of Financial Institutions

Financial Literacy Education Fund

- Removes the statutory requirement that 5% of all charges, penalties, and forfeitures paid to the Superintendent of Financial Institutions by check-cashing lenders, small loan licensees, mortgage brokers, loan officers, and certain other entities be transferred to the Financial Literacy Education Fund.
- Requires the OBM Director to transfer \$150,000 from the Consumer Finance Fund to the Financial Literacy Education Fund in each of the next two fiscal years.
- Removes the requirement that at least half of the financial literacy programs be offered at public community colleges and state institutions.
- Removes the requirement that the Director of Commerce (COM Director) provide a report to the Governor and General Assembly on such financial literacy programs.

Division of Real Estate

Real estate salesperson and broker applications

- Requires an applicant for a license as a real estate salesperson or broker to include the address of current residence on the application.
- Requires an applicant for a real estate broker license that is not an individual, to include on the application the address of the current residence of each of the applicant's members or officers.
- Exempts the addresses from the Public Records Law.

Burial permit fee

- Increases the burial permit fee from \$3.00 to \$4.50.

Division of Securities

Securities Investor Education and Enforcement Expense Fund

- Allows money in the Division of Securities Investor Education and Enforcement Expense Fund (SIEEEF) to be used for grants.
- Allows the Division of Securities to adopt rules concerning qualifications for grant-funded programs.

Ohio Investor Recovery Fund

- Removes the annual \$2.5 million cap on cash transfers from the Division of Securities Fund to the Ohio Investor Recovery Fund (OIRF).

Division of Industrial Compliance

Wage and hour records

- Requires an employer who fails to retain records related to wages and hours to pay a fine of not more than \$100 for each day the violation persists but limits the total fine to no more than \$5,000.
- Requires fines collected for failing to maintain wage and hour records to be deposited in the state treasury to the credit of the Industrial Compliance Operating Fund.

Specialty contractor license application

- Removes the requirement that a specialty contractor license application be verified by the applicant's oath (notarized).

Elevator mechanics

- Eliminates the requirement that a licensed elevator mechanic seeking a temporary continuing education waiver due to a temporary disability sign the waiver application under penalty of perjury.
- Eliminates the requirement that a physician's statements regarding the licensee's temporary disability be certified.

Board of Building Standards

Grant program

- Permits the Board of Building Standards (BBS) to establish a grant program to assist municipal, township, and county building departments ("local building departments") in recruiting, training, and retaining personnel.

Third-party plan examiners and building inspections

- Allows BBS to adopt rules that allow local building departments to accept plans examination and inspection reports from third-party building plan examiners and building inspectors.
- Permits BBS to establish competency standards for third-party building plan examiners and building inspectors.
- Specifies that the fees charged by a third-party examiner or inspector are the responsibility of the building owner and are in addition to current fees collected by local building departments on behalf of BBS.
- Clarifies that plan approvals and certificates of occupancy or completion remain the exclusive authority of the certified personnel employed by or under contract with a certified local building department and cannot be issued by a third-party examiner or inspector.

Residential building code enforcement

- Separates the state’s Residential Building Code into two distinct categories of enforcement: (1) the erection and construction of new buildings, and (2) the repair and alteration of existing buildings.
- Authorizes local building departments that are certified to enforce the Residential Building Code for new buildings to also seek certification to enforce the Residential Building Code for existing buildings.
- Clarifies that local building departments and personnel are required to obtain certification from BBS for each category of the Residential Building Code they elect to enforce.
- Maintains that the 1% fee paid by certain local building departments to BBS in connection with residential buildings applies to enforcement of both categories of the Residential Building Code.

Online safety, privacy, and transparency

Kids Internet and Data Safety Commission (KIDS)

- Creates a ten-member Kids Internet and Data Safety Commission (KIDS) within the Department of Commerce (COM).
- Requires KIDS to administer and enforce the bill’s provisions concerning covered platforms, online platforms, and operators, referred to in this analysis as the Online Safety, Privacy, and Transparency Law (OSPTL).
- Allows KIDS to identify current or emerging risks of harm to children and teens associated with online platforms and recommend measures for assisting, preventing, and mitigating those harms.
- Requires KIDS to issue certain guidance to covered platforms and operators within 90 days after the effective date of the OSPTL.
- Specifies that the guidance is not binding on KIDS, covered platforms, operators, or any other person.
- Prohibits KIDS from publishing or disclosing trade secrets or information that is privileged or confidential, except to law enforcement agencies under certain specified circumstances.
- Requires KIDS to publish all other information reported under the OSPTL to the KIDS website.

Covered platforms

- Requires “covered platforms,” i.e., online platforms, video games, messaging applications, or video streaming services that are likely to be accessed by a child or teen, to take certain measures to prevent foreseeable harms to children and teens.

- Requires a covered platform to offer certain “readily accessible” and “easy-to-use” safeguards and parental controls to users that the platform knows are children or teens.
- Requires a covered platform to provide a system for reporting content harmful to children or teens and to meaningfully respond to reports within a specified period of time.
- Prohibits a covered platform from conducting market or product-focused research on children and requires a covered platform to obtain verifiable parental consent before conducting market or product-focused research on teens.
- Prohibits a covered platform from facilitating certain advertisements to children or teens and requires other advertisements to include an identifying label.
- Requires a covered platform to provide notice of the safeguards and parental tools to children and teens and, in the case of a child, obtain verifiable parental consent.
- Requires a covered platform to explain any personalized recommendation systems it uses and to provide the opportunity for children, teens, and their parents to opt out of such systems.
- Requires covered platforms with more than 350,000 active Ohio users per month to undergo third-party audits and issue annual reports concerning compliance with the OSPTL.

Online platforms

- Requires “online platforms,” i.e., a public website, online service, online application, or mobile application that provides a community forum for user generated content, to provide notices about the algorithms used to display content on the platform and to allow users to opt into an input-transparent algorithm.

Operators

- Prohibits certain practices by operators of websites, online services, online applications, and mobile applications related to collection, use, disclosure, and retention of personal information of children and teens.
- Requires such operators to obtain “verifiable consent” from the teen or the parent of the child before collecting such personal information, subject to certain exclusions.
- Prohibits an operator from collecting, using, disclosing, or maintaining a child’s or teen’s personal information for the purposes of delivering individual-specific advertising.
- Prohibits an operator from using personal information collected to support the internal operations of a website, online service, online application, or mobile application for any other purpose.
- Prohibits an operator from conditioning a child’s or teen’s participation in a game, a prize, or any other activity on disclosing more personal information than is reasonably necessary for such participation.

- Requires an operator to provide notice what personal information the operator collects from children and teens, how the operator uses that information, the operator's disclosure practices, the opportunities available to correct or delete the information, and the procedures and mechanisms the operator uses to comply with the OSPTL.
- Requires an operator to provide opportunities to obtain personal information collected by the operator, correct inaccurate personal information, and opt out of future collection, use, and maintenance of personal information.
- Requires an operator to obtain verifiable consent from a teen or the parent of a child before collecting, using, or disclosing that teen's or child's personal information.
- Requires an operator to establish, implement, and maintain reasonable security practices to protect the confidentiality, integrity, and accessibility of personal information the operator collects from children and teens.
- Permits KIDS to allow a common verifiable consent mechanism that may be used to allow a teen or the parent of the child to grant consent for multiple websites, online platforms, online applications, and mobile applications.
- Allows an operator to submit self-regulatory guidelines to KIDS that, if approved, would demonstrate compliance with all elements of the OSPTL.

Enforcement and penalties

- Requires all actions enforcing the OSPTL to identify a violation of a specific statute or rule, as opposed to a violation of guidelines issued by KIDS.
- Allows KIDS to impose administrative penalties on persons not in compliance with the OSPTL.
- Requires KIDS to allow a grace period for persons in substantial compliance with the OSPTL and who correct the violation within 90 days.
- Requires all administrative penalties to be deposited to the Kids Internet and Data Safety Fund, to be used by KIDS to enforce the OSPTL, and by the Director of Behavioral Health to support online addiction treatment for minors.

Effective date

- Delays the effective date of the OSPTL until July 1, 2026.

Division of Unclaimed Funds

- Authorizes COM to exchange information with political subdivisions and other state agencies to locate and return unclaimed funds to their rightful owner.
- Authorizes COM to waive the submission of the standard claim form under certain specified circumstances.
- Establishes guidelines relating to claims made by and paid to a deceased owner's estate.

- Imposes 3% interest on unclaimed funds that are not timely reported, paid, or delivered, and an additional \$100-per-day penalty after four months.
- Allows the COM Director to waive interest charges upon a showing of good cause.
- Eliminates the requirement that the value of intangible property be determined, for the purposes of unclaimed funds penalties, based on market value or by the method used by the Department of Taxation.
- Specifies that the fine for other violations of the Unclaimed Funds Law is not more than \$500 per offense, is in lieu of the penalties and interest for failing to report, pay, or deliver unclaimed funds, and may be waived by the Director if the person acted in good faith and without negligence.
- Allows the Director to impose an additional civil penalty for filing a fraudulent unclaimed funds report.

Division of Liquor Control

Spirituos liquor sales

- Clarifies that the Division has authority to sell spirituous liquor from A-3a liquor permit premises (micro-distilleries) because, under current law, those permit holders sell spirituous liquor that the permit holder manufactures under contract with the Division.

Liquor permit fee changes

- Stipulates that the fee for the D-7 liquor permit (restaurants and bars located in a resort area), which is issued for six months, is \$2,814, rather than \$469 per month; thus the fee is the same over the six-month period.
- For purposes of the current \$60 per day F-4 liquor permit fee (for wine festivals one to three days long), increases or retains the fee depending on the number of days of the festival.
- For purposes of the current \$60 per day F-11 liquor permit fee (for craft beer festivals one to three days long), increases or retains the fee depending on the number of days of the festival.
- Transfers deposits of H liquor permit fees derived from permit holders whose permit premises are located outside Ohio from the existing Undivided Liquor Permit Fund to the existing State Liquor Regulatory Fund.
- Increases from \$100 to \$250 the fee for the renewal of an S-2 liquor permit (large winery), thus making the amount of the renewal fee equal to the \$250 fee for an initial S-2 liquor permit.

Division of Financial Institutions

Financial Literacy Education Fund

(R.C. 121.085 and 1321.21; Sections 243.10 and 243.30)

The bill removes the requirement that the OBM Director transfer 5% of the charges, penalties, and forfeitures paid to the Superintendent of Financial Institutions by check-cashing lenders, small loan licensees, mortgage brokers, loan officers, and certain other entities regulated by the Superintendent, from the Consumer Finance Fund to the Financial Literacy Education Fund. The Consumer Finance Fund remains the only source of revenue for the Financial Literacy Education Fund. The bill requires the OBM Director to transfer up to \$150,000 from the consumer finance fund to the Financial Literacy Education Fund in each of the next two fiscal years. Under continuing law, the remaining money in the Consumer Finance Fund is used to defray the costs of regulating the above-mentioned entities.

The bill removes the requirement for the Director of Commerce (COM Director) to adopt a rule requiring at least half of the financial literacy education fund programs to be offered at public community colleges and state institutions. It also removes a requirement that the Director provide an annual report to the Governor and the leadership of the House of Representatives and the Senate that outlines each financial literacy education program developed or implemented, the number of individuals educated by the program, and the accounting for all funds distributed.

Division of Real Estate

Real estate salesperson and broker applications

(R.C. 4735.06 and 4735.09)

Continuing law requires that real estate salespersons and brokers obtain a license from the Superintendent of the Division of Real Estate and Professional Licensing within the Department of Commerce (COM). The bill requires the applicant for a real estate salesperson or broker license to include on the application the address of the applicant's current residence. In the case of a real estate broker, which can be an individual or a business, the bill requires that if the applicant is not an individual, the application must include the address of the current residence of each of the applicant's members or officers. The bill specifies that the address information is not subject to Ohio's Public Records Law.²⁷

Burial permit fee

(R.C. 3705.17)

The bill increases the burial permit fee from \$3.00 to \$4.50. Under continuing law, when obtaining a burial permit, a funeral director or other person must pay a fee to the local registrar or sub-registrar. The local registrar or sub-registrar that issues the burial permit retains 50¢. The remainder is paid to the Cemetery Registration Fund and used to maintain operations of the

²⁷ R.C. 4735.06(A)(3) and (4) and 4735.09(A).

Division of Real Estate and Professional Licensing and the Cemetery Dispute Resolution Association.

Division of Securities

Securities Investor Education and Enforcement Expense Fund

(R.C. 1707.37)

The bill expands the purposes for which money in the Division of Securities Investor Education and Enforcement Expense Fund (SIEEEF) to be used to fund grants, in addition to paying expenses for education and protection of securities investors and the public. The bill also expands the Division's rulemaking authority to allow for rules concerning qualifications for grant-funded programs.

Ohio Investor Recovery Fund

(R.C. 1707.47)

The bill removes the \$2.5 million annual cap on transfers from the Division of Securities to the Ohio Investor Recovery Fund (OIRF). Under continuing law, the OIRF provides restitution to individuals, businesses, and organizations domiciled in Ohio that are victims of securities fraud. The maximum OIRF award is limited to the lesser of \$25,000 or 25% of the monetary injury suffered by the victim according to a final administrative order issued by the Division. To receive a restitution assistance award, a claimant must submit an application to the Division within 180 days after the date of the final order.

Division of Industrial Compliance

Wage and hour records

(R.C. 121.084 and 4111.99)

The bill requires an employer who fails to retain records related to wage rates, wages paid, and hours worked by each employee to pay a fine of not more than \$100 for each day the violation persists. However, total fines assessed on an employer for the failure may not exceed \$5,000. Fines collected for recordkeeping violations must be paid into the state treasury to the credit of the Industrial Compliance Operating Fund. Under continuing law, COM uses the fund to pay the Division of Industrial Compliance's operating expenses and the Division's share of the COM's administrative costs.

The Minimum Wage Amendment to the Ohio Constitution and Ohio's Minimum Fair Wage Standards Law require an employer to make a record of all the following for each employee and keep the records for a period of not less than three years after the employee's employment ends:

- The name, address, and occupation of the employee;
- The rate of pay and the amount paid to the employee;
- The hours worked each day and each work week by the employee;

- Any other information the Director prescribes by rule as necessary or appropriate for enforcing the overtime law.

An employer must, on request and without charge, provide the information to an employee or a person acting on behalf of the employee. The employer also must make the records available for inspection or copying by the COM Director at any reasonable time.²⁸

Specialty contractor license application

(R.C. 4740.06)

The bill removes the requirement that a specialty contractor license application be verified by the applicant's oath. Under current law, the application must be notarized. A specialty contractor license is required to be one of the following types of commercial contractor: heating, ventilating, and air conditioning (HVAC) contractor; refrigeration contractor; electrical contractor; plumbing contractor; or hydronics contractor.

Elevator mechanics

(R.C. 4785.041; Section 125.10)

Under continuing law, a licensed elevator mechanic who is unable to complete the continuing education required to renew a license due to a temporary disability may apply to place the license on inactive status. The bill eliminates the requirements:

- That the licensee sign the application under penalty of perjury; and
- That the accompanying physician statement attesting to the temporary disability be certified.

To reactivate the license, the licensee must submit another physician statement attesting that the temporary disability has ended. The bill eliminates the requirement that the physician statement be certified.

Board of Building Standards

Grant program

(R.C. 3781.10 and 3781.102)

Under continuing law, the Ohio Board of Building Standards (BBS) within COM is in charge of adopting the state building codes as well as certifying municipal, township, and county building departments ("local building departments") and their personnel throughout Ohio to enforce the state building codes. The bill permits BBS to establish a grant program to assist local building departments in the recruitment, training, and retention of qualified personnel. The grant program is funded using fees credited to the Industrial Compliance Operating Fund in connection with inspections and approval of plans and specifications by local building departments.

²⁸ R.C. 4111.08 and 4111.14(F), not in the bill; see also Ohio Constitution, Article II, Section 34a.

Third-party plan examiners and building inspections

(R.C. 3781.10)

Under current law, only certified local building departments and personnel are authorized to exercise enforcement authority respecting the state building codes. The bill allows BBS to adopt rules authorizing certified local building departments to accept plans examination and inspection reports from a third-party examiner or inspector.

The rules may require the third-party examiner or inspector to obtain certification from BBS or “to demonstrate equivalent competency” as specified and determined by BBS. The bill does not necessarily require that a third-party examiner or inspector be certified or trained in the same manner as local building department personnel. The bill specifies that the fees charged by a third-party examiner or inspector are in addition to the fees collected by the local building department on behalf of BBS. Furthermore, any additional fee for the third-party inspection is the responsibility of the building owner.

The bill clarifies that plan approvals and certificates of occupancy or completion remain the exclusive authority of the certified personnel employed by or under contract with a certified local building department. Such approvals and certificates cannot be issued by a third-party examiner or inspector.

Divide Residential Building Code

(R.C. 3781.10 and 3781.102)

Ohio has two building codes: one for *nonresidential buildings* (a building that is not a residential building or a manufactured or mobile home), and one for *residential buildings* (a one-family, two-family, or three-family dwelling house, and any accessory structure incidental to that dwelling house, but not an industrialized unit or a manufactured or mobile home).²⁹ The codes are adopted pursuant to the Building Standards Law.³⁰ Under current law, changed in part by the bill, the Residential Building Code provides uniform requirements for residential buildings in any area with a certified local building department. The bill divides enforcement of the Residential Building Code into two distinct categories:

1. The erection and construction of new residential buildings;
2. The repair and alteration of existing residential buildings.

Under the bill, a local building department and its personnel may seek certification to enforce only the Residential Building Code for new buildings, or to enforce the Residential Building Code for both new buildings and existing buildings. These are separate certifications through BBS. Under continuing law, local building departments collect a 1% fee from building owners on behalf of BBS when the local building department accepts and approves plans and

²⁹ R.C. 3781.06.

³⁰ R.C. Chapters 3781 and 3791.

conducts inspections. The bill maintains that 1% fee and applies it to both new and existing residential building enforcement.

Online safety, privacy, and transparency

Kids Internet and Data Safety Commission (KIDS)

(R.C. 3793.02, 3793.03, 3793.04, and 3793.05)

Composition

The bill creates the Kids Internet and Data Safety Commission (KIDS) within COM, consisting of the following ten members:

- One member appointed by the President of the Senate;
- One member appointed by the Speaker of the House of Representatives;
- The Director of the Department of Behavioral Health, or the Director’s designee;
- The Director of Children and Youth, or the Director’s designee;
- The COM Director, or the Director’s designee;
- Five members appointed by the Governor, at least two of which have expertise in preventing online harm to children and teens.

Each member of KIDS serves at the discretion of the member’s appointing authority. The COM Director or the Director’s designee is the chair of KIDS and is responsible for calling meetings. COM and its staff are required to provide technical and administrative support as needed by KIDS.

Duties

KIDS is required to administer and enforce the bill’s provisions concerning covered platforms, online platforms, and operators, which are referred to in this analysis as the Online Safety, Privacy, and Transparency Law (OSPTL). KIDS may adopt rules as necessary to implement and enforce the OSPTL.

KIDS may also identify current or emerging risks of harm to children and teens associated with online platforms (see “**Online platforms**” below), and may recommend measures and methods for assessing, preventing, and mitigating those harms. The bill defines “child” as an individual under 13 years of age, and “teen” as an individual who is at least 13 years of age but under 17 years of age. Additionally, KIDS may recommend methods and themes for conducting research (in a variety of languages) on these harms. Furthermore, KIDS may recommend best practices and clear, consensus-based technical standards for the transparency reports and audits required by the OSPTL for covered platforms (see “**Public reports**” and “**Audits**” below). These may include methods, criteria, and scope to promote overall accountability.

Guidance

The bill requires KIDS, within 90 days after July 1, 2026, (the effective date of the OSPTL) to issue guidance concerning the application and enforcement of certain provisions of the OSPTL.

The guidance must include assistance for covered platforms and auditors (see “**Covered platforms**” and “**Audits**” below) with respect to the following:

- Identifying design features (see “**Design features**” below) that encourage or increase the frequency, time spent, or activity of children or teens on the covered platforms;
- Safeguarding children and teens against possible misuse of parental tools (see “**Parental tools**” below);
- Best practices in providing children, teens, and their parents the most protective level of control over privacy and safety (see “**Safeguards**” below);
- The use of indicia or inferences of user ages to assess use of the covered platform by children and teens;
- Methods for evaluating the efficacy of safeguards required by the OSPTL (see “**Safeguards**” below);
- The provision of additional parental tool options which allow parents to address potential harms to children and teens (see “**Parental tools**” below).

Additionally, the KIDS guidance must outline conduct which does *not* have the purpose of effect of subverting or impairing user autonomy or choice, or causing, increasing, or encouraging compulsive use for a child or teen (see “**Design features**” below). This includes the following:

- De minimis or insignificant changes to the user interface, such as different styles, layouts, or text, based on testing consumer preferences, when those changes are not done with the purpose of weakening or disabling safeguards or parental controls;
- Algorithms or data outputs outside the control of a covered platform;
- Establishing default settings that provide enhanced privacy protection to users, or which otherwise enhance their autonomy and decision-making ability.

Furthermore, KIDS must issue guidance which provides information, including best practices and examples, for understating how KIDS will determine whether an operator or covered platform knows that a user is a child or teen for the purposes of the OSPTL. Under the bill “know” is defined to include both actual knowledge and knowledge fairly implied on the basis of the circumstances. Whether a covered platform or operator knows that a user is a child or teen is determined based on “competent and reliable evidence, taking into account the totality of the circumstances, including whether a reasonable and prudent person under the circumstances would have known that the user is a child or teen.”

The bill allows, but does not require, KIDS to issue guidance to assist covered platforms in complying with notice and advertising requirements under the OSPTL. The bill specifies that the guidance issued by KIDS does not confer any rights on any person or locality. Additionally, no guidance issued by KIDS is binding on KIDS or any other person with respect to the approach recommended in that guidance.

Records

The bill prohibits KIDS from publishing or otherwise making public any trade secret or other commercial or financial information that is privileged or confidential. KIDS may only disclose privileged or confidential commercial and financial information in limited circumstances. First, it may disclose such information to officers and employees of appropriate state or federal law enforcement agencies, but only after certification by that officer, employee, or agency that the information will be maintained in confidence and used only for official law enforcement purposes. Second, it may disclose that information to an officer or employee of a foreign law enforcement agency, but only to the extent to which the Federal Trade Commission is permitted to make material available to foreign law enforcement agencies under federal law.

Otherwise, all reports and documentation submitted to KIDS under the OSPTL must be published on the KIDS website.

Covered platforms

(R.C. 3793.01, 3793.04, 3793.20, 3793.21, 3793.22, 3793.23, 3793.24, and 3793.25)

The bill requires covered platforms to adhere to certain requirements concerning design features, safeguards, and parental tools. A “covered platform” is an online platform (see “**Online platforms**” below), *online video game*, messaging application, or video streaming service that connects to the internet and that is used, or is reasonably likely to be used, by a child or teen. The definition does not include common carrier services, *broadband internet access services*, email services, video conferencing services, wireless messaging services, nonprofits, educational websites, business-to-business software, virtual private networks, or government websites.

The definition expressly includes an “online video game,” which is defined as a video game, including an educational video game, that connects to the internet and allows a user to (1) create and upload content (other than content that is incidental to game play) such as user-created character or level designs, preselected phrases, or short interactions with other users, (2) engage in *microtransactions* within the game, or (3) communicate with other users. A “microtransaction” is a purchase made in an online video game, including purchases made using virtual currency that is purchasable or redeemable using cash or credit or that is included as part of a subscription service and purchases involving surprise mechanics, new characters, or in-game items. “Microtransaction” does not include purchases using virtual currency that is earned through game play and is not otherwise purchasable or redeemable using cash or credit or included as part of a paid subscription service or purchases of additional levels within the game or an overall expansion of the game.

Expressly excluded from the definition of covered platform are “broadband internet access services” which are mass-market retail services by wire or radio that provide the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications services, but excluding dial-up internet access services.

Design features

Under the bill, covered platforms are required to take reasonable care in creating and implementing design features to prevent or mitigate certain foreseeable harms to children or teens. A “design feature” is something that encourages or increases the frequency, time spent, or activity of users on a covered platform. The term expressly includes things like infinite scrolling, autoplay, rewards or incentives, notifications, push alerts, badges or other award symbols, *personalized design features*, in-game purchases, and appearance-altering filters. A “personalized design feature” is a fully or partially automated system, including a recommendation system, that is based on the collection of personal information of users and that encourages or increases the frequency, time spent, or activity of users on the covered platform.

The duty of care applies only if a reasonable and prudent person would agree that both (1) the harm at issue is reasonably foreseeable by the covered platform, and (2) the design feature is a contributing factor to the harm. The bill identifies the following as potentially foreseeable harms to children and teens:

- Eating disorders, substance abuse disorders, and suicidal behaviors;
- “Compulsive use” of the covered platform, which the bill defines as persistent and repetitive use that significantly impacts one or more of an individual’s major life activities, including socializing, sleeping, eating, learning, reading, concentrating, communicating, or working;
- Depressive and anxiety disorders when such conditions have objectively verifiable and clinically diagnosable symptoms and are related to compulsive use of the covered platform;
- Physical violence or online harassment that is so severe, pervasive, or objectively offensive that it impacts a major life activity of a child or teen;
- “Sexual exploitation and abuse” of a child or teen, which is defined to include coercion and enticement, child sexual abuse material, trafficking for the production of images, and sex trafficking of children;
- Distribution, sale, or use of narcotics, tobacco, cannabis, alcohol, or gambling;
- Financial harms caused by unfair or deceptive acts or practices.

The bill specifies that a covered platform is not required to prevent a child or teen from independently searching for or requesting certain content, or from accessing information and resources regarding the prevention or mitigation of harms. The bill also states that a government entity is not authorized to enforce the duty of care requirement based upon the viewpoint of users expressed by or through any speech, expression, or information protected by the First Amendment to the U.S. Constitution.

Safeguards

The bill requires a covered platform to provide privacy options for users that the covered platform knows are children or teens (see “**Guidance**” above). The safeguards must include the ability to do all of the following:

- Limit the ability of other users to communicate with the child or teen;
- Prevent other users and visitors, including those who are not registered with the covered platform, from viewing the child’s or teen’s personal information (see “**Personal information**” below);
- Limit any design features that encourage or increase the frequency, time spent, or activity of children or teens on the covered platform;
- Control or opt out of personalized recommendation systems (see “**Personalized recommendation systems**” below);
- Restrict the sharing of “geolocation information,” which the bill defines as information about a user’s location that is sufficient to identify a street name and the name of a city or town;
- Limit the amount of time spent on the covered platform.

These safeguards must, by default, be set to the level that provides the highest level of protection when the covered platform knows that the user is a child or teen. The default settings may be changed by the child or teen or their parent.

Parental tools

In addition to the safeguards, a covered platform that knows a user is a child or teen must provide certain tools that allow parents to view (in the case of a teen user) or manage (in the case of a child user) privacy and account settings, restrict purchases and financial transactions, view metrics of total time spent on the covered platform, and restrict the time that may be spent on the covered platform. Furthermore, the bill requires a covered platform to provide a clear and conspicuous notice of when the tools are in effect and what settings have been applied. For a user that the covered platform knows is a child, the tools must be enabled by default. If the covered platform previously offered parental tools that meet the requirements of the OSPTL, and the parent of the child or teen user declined to enable those tools, the covered platform is not required to offer them again.

Clarity and accessibility

A covered platform must provide the safeguards and parental tools in a “readily accessible” and “easy-to-use” manner. Furthermore, the bill requires a covered platform to conspicuously provide information about the safeguards and parental tools in a manner that (1) takes into consideration the differing ages, capabilities, and developmental needs of the children and teens most likely to access the covered platform, and (2) does not encourage the child, teen, or parent to weaken or disable the privacy safeguards or parental tools. Such information must be offered in the same language, form, and manner as the product or service

provided by the covered platform and must not be designed in such a way to obscure, subvert, or impair user autonomy with respect to safeguards or parental tools.

If the covered platform is operating on behalf of an educational agency or institution, and the contract with that educational agency or institution meets the requirements, discussed below, under “**Agreements with educational agencies or institutions**,” the covered platform must provide the safeguards and parental tools to the educational agency or institution rather than the users.

The bill specifies that an online video game is not required to interrupt the natural sequence of game play, such as progressing through game levels or finishing a competition, for the purpose of complying with a safeguard or parental tool. Furthermore, if a user’s device is not connected to the internet at a time of a change to the parental tools, the covered platform is required to apply that change the next time the user’s device is connected to the internet.

Reporting harmful materials

A covered platform is required to provide a system for reporting content harmful to children or teens. The platform must respond to reports of harmful content within ten days if the platform averaged more than 350,000 active Ohio users per month during the most recent calendar year, or within 21 days if the platform averaged less than that amount of active Ohio users. Regardless of the platform’s active users, a platform is required to respond to reports involving an imminent threat to the safety of a child or teen as promptly as needed to address the threat.

Advertising and market research

The bill prohibits a covered platform from conducting market or product-focused research on users that the covered platform knows are children. Covered platforms must not conduct such research on teens unless the platform obtains verifiable parental consent from the parent of the teen prior to conducting the research (see “**Verifiable consent**” below).

Covered platforms are prohibited from facilitating advertisement of narcotic drugs, cannabis products, tobacco products, gambling, or alcohol to children or teens. Furthermore, a covered platform is required to provide clear, conspicuous, and easy-to-understand labels and information to children and teens regarding advertisements. The labels must specify (1) the name of the product, service or brand, (2) the subject matter of the advertisement, and (3) whether a particular media item is an advertisement or marketing material, including disclosure of endorsements made for consideration by users of the platform. The advertising labels may provide the required information through a link to another web page or disclosure.

Preservation of authority

The bill specifies that the design feature, safeguard, and parental tool requirements do not do any of the following:

- Prevent a covered platform from blocking, detecting, or preventing the distribution of unlawful, obscene, or other material harmful to juveniles;

- Prevent a covered platform from blocking or filtering spam, preventing criminal activity, or protecting the security of the platform;
- Require the disclosure of browsing behavior, search history, messages, contact lists, or other content or metadata of the communications of a child or teen;
- Prevent a covered platform from using a personalized recommendation system (see “**Personalized recommendation systems**” below) to display content to a child or teen if the system only uses information on the child’s or teen’s language, location, and age;
- Prevent an online video game from disclosing a username or other user identification for the purpose of competitive game play or to allow for reporting of users;
- Prevent a covered platform from contracting with a third-party entity to provide safeguards or parental tools or to offer similar or stronger protective capabilities for children or teens;
- Prevent a covered platform from cooperating with law enforcement;
- Prevent a covered platform from complying with lawful civil, criminal, or regulatory inquiries or summons;
- Prevent a covered platform from investigating and defending against legal claims;
- Prevent a covered platform from stopping, detecting, or responding to illegal activities, or investigating and reporting those responsible for illegal activities.

Video streaming services are considered to be in compliance with the design feature, safeguard, and parental tool requirements if the service is predominantly news, sports, entertainment, or other programming preselected by the provider and not user-generated, and any chat or interactive functionality is incidental to providing the content. If the service is not predominantly news or sports, the service is required to provide certain parental tools for limiting the child’s or teen’s use of the service.

Access to information

Before registering a user that the covered platform knows is a child or teen, the bill requires the platform to provide a clear, conspicuous, and easy-to-understand notice of the platform’s policies and practices with respect to safeguards for children and teens, information on how to access the required safeguards and parental tools, and, if applicable, information on the platform’s personalized recommendation system (see “**Personalized recommendation systems**” below).

Furthermore, if the platform knows that the user is a child, the platform is required to both (1) provide information to the child’s parent about the safeguards and parental tools required by the bill, and (2) obtain verifiable consent from that parent (see “**Verifiable Consent**” below). The bill authorizes a covered platform to combine these notice and consent processes with any processes that may be required by other portions of the OSPTL.

A covered platform must also provide a permanent link to comprehensive information about the safeguards and parental tools in a prominent location. All of the information and disclosures must be made available in the same language, form, and manner as the covered platform provides the product or service used by children or teens.

Personalized recommendation systems

If a covered platform operates a personalized recommendation system, the bill requires the platform's terms and conditions to include an overview of how each system is used to provide information to children and teens, how each system uses the personal information of children and teens, and information about options for children and teens, or their parents, to opt out of or control the system. The bill defines "personalized information systems" as automated systems used to suggest, promote, or rank content, including other users, hashtags, or posts, based on the user's personal information. The term excludes systems that suggest, promote, or rank content based solely on the user's language, location, or age.

Public report

The bill requires certain covered platforms to issue an annual public report based on an independent audit. The requirement applies only to covered platforms that (1) averaged more than 350,000 active Ohio users per month in the preceding calendar year, and (2) predominately provide a community forum for user-generated content and discussion. The report must be published in an easy-to-find location on a publicly available website. It must include all of the following:

- An assessment of the extent to which the covered platform is likely to be accessed by children or teens;
- A description of the commercial interests of the platform;
- The number of users that the covered platform knows are Ohio children or teens;
- The median and mean amounts of time spent on the covered platform by those children and teens on a daily, weekly, and monthly basis;
- The amount of content being accessed by those children and teens that is in English and the top five nonEnglish languages used by those children and teens;
- The total reports of materials harmful to children or teens received through the reporting mechanism required by the OSPTL, disaggregated by language (see "**Reporting harmful materials**," above);
- An assessment of the safeguards and parental tools, representations regarding the use of personal information of children and teens, and other matters of compliance;
- An assessment based on aggregate data on the exercise of safeguards and parental tools, and other competent and reliable empirical evidence;
- A description of whether and how the covered platform uses design features that increase, sustain, or extend the use of a product or service by a child or teen;

- A description of whether, how, and for what purpose the covered platform collects or processes categories of personal information (see “**Personal information**” below), including how personal information is used to operate personalized recommendation systems related to children and teens;
- An evaluation of the efficacy of safeguards and parental tools required by the bill, and any issues in delivering them;
- A description of the safeguards and parental tools available to children, teens, and parents on the covered platform;
- A description of the prevention and mitigation measures a covered platform may take, if any, in response to the assessments conducted as part of the report, including steps taken to provide the most protective level of control over safety by default;
- A description of the processes used for the creation and implementation of any design feature that will be used by children or teens;
- A description and assessment of handling reports of materials harmful to children or teens, including the rate of response, timeliness, and substantiveness of responses;
- The status of implementing prevention and mitigation measures identified in prior assessments.

When issuing the report, the covered platform must take steps to safeguard the privacy of its users, including by ensuring that data is presented in a de-identified, aggregated format such that it is not reasonably linkable to any user. The bill defines “de-identified” as data that does not identify and is not linked or reasonably linkable to a device that is linked or reasonably linkable to an individual, regardless of whether the information is aggregated.

Audits

The bill requires the independent, third-party auditor to do all of the following in conducting an inspection of the reasonably foreseeable risk of harm to children or teens:

- Take into consideration the function of personalized recommendation systems;
- Consult parents and youth experts, including youth and families with relevant past or current experience, public health and mental health nonprofit organizations, health and development organizations, and civil society with respect to the prevention of harms to children or teens;
- Conduct research based on experiences of children and teens that use the covered platform, including reports from the reporting system required by the OSPTL and information provided by law enforcement;
- Take account of research, including research regarding design features, marketing, or product integrity, industry best practices, or outside research;
- Take into consideration indicia or inferences of age of users, in addition to any self-declared information about the age of users;

- Take into consideration differences in risk of reasonably foreseeable harms and effectiveness of safeguards across English and non-English languages.

The covered platform is required to facilitate the audit by providing the third-party auditor all information and material relevant to the audit, make available all networks, systems, and assets relevant to the audit, and disclose all facts relevant to the audit.

Online platforms

(R.C. 3793.01 and 3793.30)

The bill also establishes transparency requirements for online platforms that use opaque algorithms. Under the bill, an “online platform” is any public-facing website, online service, *online application*, or *mobile application* that predominantly provides a community forum for user generated content, such as sharing videos, images, games, audio files, or other content, including a social media service, social network, or virtual reality environment. Websites, services, and applications are not considered online platforms solely on the basis of including incidental chat or comment functions. Websites, services, and applications with the predominate purpose of providing travel reviews are expressly excluded from the definition.

An “online application” is an internet-connected software program, including a service or application offered via a connected device. A “mobile application” is a software program that runs on the operating system of a cell phone, tablet, or similar portable computing device that transmits data over a wireless connection. The term includes services or applications offered via a connected device.

Algorithms

Generally speaking, an “algorithmic ranking system” is a computational process used to determine the selection, order relative prioritization, or relative prominence of content from a set of information that is provided to a user on an online platform, including the ranking of search results, the provision of content recommendations, the display of social media posts, or any other method of automated content selection. The term includes computational processes derived from algorithmic decision making, machine learning, statistical analysis, or other data processing or artificial intelligence techniques.

An “opaque algorithm” is an algorithmic ranking system which determines the order or prominence in which information or content is displayed to a user based, in whole or in part, on user-specific data that was not expressly provided by the user to the platform for that purpose. This data could include personal information attached to the account, inferences about the users, as well as other data such as online identifiers like site or advertising cookies which track a user’s online habits or presumed preferences.

Alternatively, an “input-transparent algorithm” means a ranking algorithm that does not use user-specific data to determine the order or prominence in which information or content is displayed to a user, unless the user expressly provides that data to the platform *for that purpose*. Even when a user does expressly provide data for that purpose, it only applies to limited types of user-specific data, such as search terms, filters, saved preferences, approximate geolocation information (i.e., information that identifies location to a precision of less than five miles), and

data submitted to express the user’s desire to receive particular information, such as subscribing to or following accounts on social media. This data does *not* include the user’s device history, web search and browsing history, previous geographical locations, physical activity, device interactions, financial transactions, or inferences about the user or the user’s connected device.

Transparency requirements

The bill requires online platforms that use opaque algorithms to provide users with clear and conspicuous notice that the platform applies user-specific data to select the content the user sees. The notice must be provided whenever the user interacts with an opaque algorithm for the first time. It may be a one-time notice that may be dismissed by the user.

In addition, the online platform must include all of the following information in its terms and conditions:

- The most salient features, inputs, and parameters used by the opaque algorithm;
- How any user-specific data used by the algorithm is collected or inferred about a user of the online platform, and the categories of such data;
- Any options that the online platform makes available for a user of the platform to opt out or exercise options under this section, modify the profile of the user, or to influence the features, inputs, or parameters used by the algorithm;
- Any quantities, such as time spent using a product or specific measures of engagement or social interaction, that the algorithm is designed to optimize, as well as a general description of the relative importance of each quantity for such ranking.

The notice must be displayed in a clear, accessible, and easily comprehensible manner. It must be updated whenever the online platform makes a material change to the opaque algorithm. If the online platform is operating on behalf of an educational agency or institution, and the contract with that educational agency or institution meets the requirements, discussed below, under “**Agreements with educational agencies or institutions,**” the online platform must provide the required notices to the educational agency or institution rather than the users.

Ability to switch

An online platform that uses an opaque algorithm must allow users to easily switch between that algorithm and an input-transparent algorithm. The bill prohibits an online platform from charging users different rates or otherwise discriminating against them based on their choice in algorithm.

Confidential information

The bill specifies that online platforms are not required to disclose trade secrets, confidential business information, or privileged information.

Operators

(R.C. 3793.01, 3793.04, 3793.40, 3793.41, 3793.42, 3793.43, 3793.44, 3793.45, 3793.46, and 3793.47)

The bill also regulates the data collection and processing practices of operators of websites, online services, online applications, and mobile applications. An “operator” is a person who, for commercial purposes, operates or provides a website, online service, online application, or mobile application, and collects or maintains, either directly or through a service provider, personal information from or about users of that website, online service, online application, or mobile application. The term includes a person that allows another person to collect personal information directly from users or allows users to publicly disclose personal information. Nonprofit corporations and unincorporated nonprofit organizations, existing under the laws of Ohio or any other state, are not included in the definition.

Scope

The OSPTL applies to an operator only if (1) the website, online service, online application, or mobile application is directed to children, or (2) the operator knows (see “**Guidance**” above) that a particular user of the website, online service, online application, or mobile application is a child or teen.

The bill requires KIDS to determine whether a particular website, online service, online application, mobile application, or any portion thereof, is “directed to children.” That determination must be based on the totality of circumstances, taking into consideration competent and reliable empirical evidence regarding the composition of the *actual* audience of the website, online service, online application, or mobile application, as well as evidence regarding the *intended* audience. The bill specifies that a website, online service, online application, or mobile application is not directed to children merely because it links users to another site, service, or application that is directed to children by using information location tools, a directory, index, reference, pointer, or hypertext link.

Personal information

The bill defines “personal information” as individually identifiable information about an individual collected online, including first a last name; home or other address; email address; telephone number; Social Security number; a photograph, video, or audio file containing an individual’s image or likeness; geolocation information; biometric data such as fingerprints, voice prints, or facial templates; persistent identifiers like an internet protocol address; or any other information that allows for an individual to be contacted. The term excludes information used by the operator solely for providing internal operations support and certain voice data.

Individual-specific advertising

The bill prohibits an operator from collecting, using, *disclosing* to third parties, or maintaining the personal information of the child or teen for the purposes of delivering individual-specific advertising, or from allowing another person to do the same. “Individual-specific advertising” is defined as marketing a product or service in a manner directed to a specific child or teen, or a *connected device* that is linked (or reasonably linkable) to a child or teen, based

on personal information, profiling, or unique identifiers associated with a connected device. The term excludes advertising in response to a user's specific request for information, contextual advertising, and processing personal information solely for measuring or reporting advertising or content performance, reach, or frequency.

The bill defines "connected device" as a device that is capable of connecting to the internet; has computer processing capabilities for collecting, sending, receiving, or analyzing data; and is primarily designed for or marketed to consumers.

The bill defines "disclosure" either (1) releasing personal information collected from a child or teen for any purposes other than the provision of support for the internal operations of the website, online service, online application, or mobile application (see "**Collection, storage, and use of personal information**" below), or (2) making personal information collected from a child or teen publicly available in an identifiable form, including by a public posting through the internet or through the home page of a website, a pen pal service, an email service, a message board, or a chat room.

Collection, storage, and use of personal information

The bill prohibits an operator from collecting personal information from a child or teen, except when the collection is consistent with either the context of a particular transaction or service, or the relationship of the child or teen with the operator. The bill expressly preserves the ability of an operator to collect personal information that is necessary for the operator to fulfill a transaction or provide a product or service requested by the child or teen. The bill also preserves the ability of an operator to collect personal information when the operator is required or specifically authorized to do so by law.

Under the bill, an operator is prohibited from retaining the personal information of a child or teen for longer than is reasonably necessary to fulfill a transaction or provide a service requested by the child or teen, except as required or specifically authorized by law. Furthermore, the bill prohibits an operator from storing or transferring the personal information of a child or teen outside of Ohio unless the operator first provides direct notice to a parent of the child, in the case of a child, or the teen, in the case of a teen.

If an operator collects the personal information of a child or teen for the *support of the internal operations of the website, online service, online application, or mobile application*, the operator must not use or disclose that information for any other purpose. Under the bill, "support for the internal operations of a website, online service, online application, or mobile application" means activities necessary to maintain or analyze functioning, perform network communications, authenticate users, personalize content, serve contextual advertising, protect security and integrity, ensure legal or regulatory compliance, or fulfill the request of a child or teen where verifiable consent is not required. The bill specifically disallows using personal information collected for that purpose to do any of the following:

- Contact a specific individual, including through individual-specific advertising;
- Amass a profile on a specific individual;
- Encourage or prompt use of a website or online service.

Conditions of participation

The bill prohibits an operator from conditioning a child's or teen's participation in a game, a prize, or any other activity disclosing more personal information than is reasonably necessary to participate in the game, prize, or activity.

Notices

The bill also requires operators to provide clear and conspicuous notice of all of the following:

- What personal information the operator collects from children and teens;
- How the operator uses the information;
- The operator's disclosure practices for the information;
- The purposes for which the operator collects, uses, discloses, and retains the information;
- The rights and opportunities available to correct or delete the information;
- The procedures or mechanisms the operator uses to ensure compliance with the OSPTL.

Verifiable consent

Before an operator can collect, use, or disclose the personal information of a child or teen, the bill requires the operator to obtain verifiable consent from the parent of the child or from the teen. If the purpose of collecting or disclosing the data is materially different from that specified when verifiable consent was last obtained, the operator is required to obtain verifiable consent for the new purpose. The bill defines "verifiable consent" as making a reasonable effort to ensure that the user or, in this case, the user's parents receives direct notice of the personal information use, collection, and disclosure practices of the platform, and that the user or the user's parents clearly authorizes that collection, use, and disclosure before the platform collects any personal information.

Disclosures and opportunities

The bill requires an operator to provide certain disclosures and opportunities to a teen or the parent of a child, upon request and proper identification. In the case of the parent of the child, the operator must provide the following:

- A description of the specific types of personal information the operator collects from the child;
- The opportunity to delete personal information collected from or content submitted by the child;
- The opportunity to refuse to permit the operator's further collection of personal information from the child or the further use and maintenance of personal information already collected from the child;
- The opportunity to challenge the accuracy of the child's personal information and, if the parent establishes the inaccuracy of such personal information, to correct the inaccuracy;

- A means that is reasonable under the circumstances for the parent to obtain any personal information collected from the child if such personal information is available to the operator at the time the parent makes the request.

In the case of a teen, the operator must provide the following:

- A description of the specific types of personal information the operator collects from the teen, the method by which the operator obtains the personal information, and the purposes for which the operator collects, uses, discloses, and retains the personal information;
- The opportunity to delete personal information collected from or content submitted by the teen;
- The opportunity to refuse to permit the operator's further collection of personal information from the teen or the further use and maintenance of personal information already collected from the teen;
- The opportunity to challenge the accuracy of the teen's personal information and, if the teen establishes the inaccuracy of such personal information, to correct the inaccuracy;
- A means that is reasonable under the circumstances for the teen to obtain any personal information collected from the teen, if such information is available to the operator at the time the teen makes the request.

The bill permits an operator to terminate service provided to a child whose parent has refused, or a teen who has refused, to permit the operator's further collection, use, or maintenance of personal information from that child or teen, but only to the extent that the operator is incapable of providing the service without such information. In other words, an operator cannot discontinue service following such a request if it is still capable of providing the service without that collected information.

Security practices

An operator must establish, implement, and maintain reasonable security practices that will protect the confidentiality, integrity, and accessibility of personal information of children or teens collected by the operator. Furthermore, the operator must protect that personal information against unauthorized access.

Preservation of authority

An operator and its agents are shielded from penalties respecting disclosures made in good faith in response to a request made by the parent of a child or by a teen. Additionally, the bill does not prohibit an operator that knows that a user is a child or a teen from delivering advertising or marketing that is age-appropriate, so long as the operator does not use any information other than the fact that the user is a child or a teen.

Furthermore, the bill specifies that a request to delete or correct personal information does not limit the authority of a law enforcement agency to lawfully obtain any content or information from the operator, require the operator to delete information submitted by a person

other than the user trying to erase the information or content. Nor does the bill prohibit an operator from retaining a record of a deletion request and the minimum necessary information for the purposes of ensuring compliance with the request, preventing detecting, protecting against, responding to, or reporting security incidents, protecting the integrity of the operator's website or online service, or ensuring that the child or teen's personal information remains deleted.

Common verifiable consent mechanism

Under the bill, KIDS may allow operators to use a common verifiable consent mechanism that fully meets the requirements of the OSPTL. In assessing a common verifiable consent mechanism, KIDS must consider whether a single operator could use the mechanism to obtain verifiable consent from a parent of a child or teen on behalf of multiple listed operators that provide a joint or related service. In other words, once verifiable consent has been provided to a common verifiable consent mechanism, it will function as verifiable consent for all listed operators providing joint or related services who use that common mechanism. If KIDS allows the use of a common verifiable consent mechanism, the bill requires it to adopt rules which permit that use.

Self-regulatory guidelines

The bill provides that an operator may satisfy all of the requirements of the OSPTL, as well as any related rules promulgated by KIDS, by following self-regulatory guidelines issued by representatives of the marketing or online industries and approved by KIDS. After a request to approve self-regulatory guidelines, KIDS must provide, in writing, its conclusions regarding that request within 180 days.

Exemptions

The bill provides several scenarios where an operator is not required to obtain verifiable consent from a teen or the parent of a child prior to collecting personal information from that teen or child:

- Online contact information collected from a child or teen that is used only to respond directly on a one-time basis to a specific request from the child or teen; is not used to recontact the child or teen or to contact another child or teen; and is not maintained in retrievable form by the operator;
- A request for the name or online contact information of a parent or teen that is used for the sole purpose of obtaining verifiable consent and where, if verifiable consent is not obtained after a reasonable period of time, the information is not maintained in retrievable form by the operator;
- Online contact information collected from a child or teen that is used only to respond more than once directly to a specific request from the child or teen, is not used to recontact the child or teen beyond the scope of that request, if reasonable efforts are used to notify the parent or teen of the information collected and to offer the opportunity to request that the operator make no further use of the information, or in situations otherwise determined to be acceptable by the KIDS Commission.

- The name of the child or teen and online contact information to the extent reasonably necessary to protect the safety of a child or teen participant on the website, online service, online application, or mobile application if the information is only used for that purpose and opportunity is provided to request that the operator make no further use of the information.
- The collection, use, or dissemination of personal information by the operator necessary to protect the security or integrity of the operator's platform, to take precautions against liability, to respond to judicial process, and to the extent otherwise permitted by law to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

Agreements with education agencies or institutions

Additionally, KIDS may adopt rules which provide that verifiable consent is not required when an operator is acting under a written agreement with an education agency or institution. In that case, the written agreement must require, at a minimum, all of the following:

- The operator to limit its collection, use, and disclosure of the personal information from a child or teen to solely educational purposes;
- The operator to provide the educational agency or institution with a notice of the specific types of personal information that the operator will collect, the method by which it will obtain that information, and the purposes for which it will collect, use, disclose, and retain the information;
- The operator to provide the educational agency or institution with a link to the operator's online notice of information practices;
- Upon request, the operator to provide to the educational agency or institution with a means to review the personal information collected from a child or teen, to prevent further use, maintenance, or future collection of a child's or teen's personal information or content submitted to the operator's website, online service, or online or mobile application;
- The representative of the educational agency or institution to acknowledge and agree that the representative has the authority to authorize the collection, use, and disclosure of personal information from children or teens on behalf of the educational agency or institution, and provide the representative's name and title at the educational agency or institution;
- The educational agency or institution to provide a notice on its website that identifies the operator with which the educational agency or institution has entered into a written agreement and a link to the operator's notice of information practices;
- Upon request, the educational agency or institution to provide the operator's notice regarding information practices to a parent, in the case of a child, or a parent or teen, in the case of a teen;

- Upon the request of a parent, in the case of a child, or a parent or teen, in the case of a teen, the educational agency or institution to provide a means to review the personal information collected from the child or teen and provide that parent or teen a means to review the personal information.

Enforcement and penalties

(R.C. 3793.04, 3793.06, and 3793.90)

Enforcement actions

Any enforcement action under the OSPTL must allege a specific violation of a statute or rule. No enforcement action or consent order may be based on practices that are alleged to be inconsistent with any guidance issued by KIDS, unless those practices also violate a statute or rule.

Penalties

KIDS may impose an administrative penalty on any operator, covered platform, online platform, or other person that KIDS determines has failed to comply with the OSPTL. The amount of the penalty is determined as follows:

- Up to \$1,000 per day for the first 60 days;
- Up to \$5,000 per day for day 61 to 90;
- Up to \$10,000 per day for day 91 and thereafter.

However, the bill provides a grace period during which administrative penalties can be avoided. If an operator, covered platform, online platform, or other person is in substantial compliance with the OSPTL, then KIDS must provide written notice to the violator before imposing any administrative penalties. This notice must identify the specific provisions that have been violated. If, within 90 days after the date the notice is sent, the violator cures the violation and provides KIDS with written documentation that the violation has been cured and that it has taken measures sufficient to prevent future violations, then KIDS must not impose an administrative penalty.

All administrative penalties collected must be deposited into the Kids Internet and Data Safety Fund. If the administrative penalty is not paid within 90 days after it is imposed, KIDS may file a civil action in the Court of Common Pleas of Franklin County to enforce the penalty. Violators are also liable for any costs incurred by KIDS in conducting an investigation and bringing an action.

Kids Internet and Data Safety Fund

The bill creates the Kids Internet and Data Safety Fund within the state treasury. This fund consists of all administrative penalties collected for violations of the OSPTL, as well as all investment earnings of the fund. KIDS must use the money in the fund for its own expenses and for administering and enforcing the OSPTL. In addition, the Director of Behavioral Health may use any unencumbered funds to support online addiction treatment for minors, which will be administered by DBH.

Effective date

(Section 820.40)

The OSPTL takes effect July 1, 2026.

First and Fourteenth Amendment considerations

The OSPTL could be challenged under the First and Fourteenth Amendments to the U.S. Constitution. The U.S. District Court for the Southern District of Ohio enjoined enforcement of a similar Ohio law, enacted by H.B. 33 of the 135th General Assembly in 2023, that requires operators of social media websites to obtain “verifiable consent” from a parent or guardian before allowing an Ohio resident under age 16 to create an account. The court held that the H.B. 33 provisions are content-based and subject to strict scrutiny under the First Amendment. Furthermore, the court indicated that the H.B. 33 provisions could be void for vagueness under the Due Process Clause Fourteenth Amendment.³¹

Division of Unclaimed Funds

Background

The Unclaimed Funds Law (1) specifies the types of funds that are “unclaimed,” (2) requires holders of such funds to report them to the COM Director, give notice to the owners or beneficiaries, and pay a portion of the funds to the Director, and (3) requires the Director annually to publish notice of the funds in the appropriate county. Unclaimed funds that are paid to the Director do not become the property of the state, but are held in the Unclaimed Funds Trust Fund until claimed by the owner.³²

Exchanging information

(R.C. 169.061)

The bill authorizes the Director to exchange information with any state officer, board, or commission, or any political subdivision, to assist the Director in performing duties under the Unclaimed Funds Law. Such information may include records related to the notice, report, remission, and return of unclaimed funds to a rightful claimant.

Waiving the claim form

(R.C. 169.08)

Under continuing law, changed in part by the bill, the Director must pay the owner or other person who has established the right to unclaimed funds after such owner or person files a claim form with the Director.³³ The bill allows the Director to waive submission of the claim form if the claimant is listed as the owner of the funds on the report submitted to COM by the holder and the Director reasonably believes the claimant is entitled to receive payment. The bill

³¹ *NetChoice, LLC v. Yost*, S.D. Ohio, No. 2:24-cv-0047, 2024 U.S. Dist. LEXIS 24129 (February 12, 2024).

³² R.C. Chapter 169.

³³ R.C. 169.03, not in the bill.

authorizes the Director to use state tax information and information from reliable databases of the Director's choosing to assist in determining whether a claimant is entitled to payment.

Deceased owners

(R.C. 169.081)

The bill prohibits the Director from authorizing a payment from the Unclaimed Funds Trust Fund when the claimant is the representative of a deceased owner's estate, or another person related to a deceased owner's estate, unless it affirmatively appears to the Director that the payment of the unclaimed funds will go to (1) the actual heirs or legatees of the deceased owner, or (2) creditors of the deceased owner that are valid and not barred.

In addition, the bill specifies that the amount received from the Unclaimed Funds Trust Fund by a creditor for a claim relating to the administration of the deceased owner's estate must not exceed the reasonable cost of administering the estate, including court costs, administration fees, and attorney's fees. For other creditors, the amount received must not exceed the amount necessary to pay the creditor's claim, excluding any claim or portion of a claim that is not in existence on the date of the owner's death.

This deceased owner provisions apply to claims filed and pending on and after the bill's 90-day effective date.

Penalties for failing to report, pay, or deliver funds

(R.C. 169.12)

Under current law, a holder of unclaimed funds is subject to a \$100-per-day civil penalty for knowingly failing to report unclaimed funds to COM. An additional \$100-per-day penalty applies if the holder fails to report the unclaimed funds within four months after receiving a request from the Director. If the unclaimed funds are not timely paid, interest applies at either the best available, nonnegotiable, retail time deposit base rate offered by the holder, if the holder is a financial institution, or, otherwise, at the best available six-month treasury bill rate offered in the calendar year preceding discovery of the violation. Furthermore, a civil penalty of 1% of the unpaid amount applies each month, for up to 25 months.

The bill instead imposes 3% annual interest on unclaimed funds that are not timely reported, paid, or delivered to COM. An additional \$100-per-day civil penalty, up to \$10,000, applies if the holder fails to report, pay, or deliver the unclaimed funds within four months after the date required by law.

Under continuing law, the Director may waive the civil penalties for good cause and is required to waive them upon a showing that a holder had reasonable grounds for not complying with the Unclaimed Funds Law. The bill also permits the Director to waive interest upon a showing of good cause.

The bill eliminates the current law requirement that the value of unclaimed funds that are intangible property, for the purpose of determining the amount of interest and penalties, be determined based on the market value as of the date for reporting and payment or, if no market value is determinable, on the basis used by the Department of Taxation.

Other penalties

(R.C. 169.99)

Under current law, a person who knowingly violates the Unclaimed Funds Law is subject to a fine of not more than \$500. The bill specifies that the fine is \$500 per offense. Furthermore, the bill provides that the fine is in lieu of, not in addition to, the penalties and interest described above for failing to timely report, pay, or deliver unclaimed funds. The bill permits the Director to waive the penalty if the Director finds that the person fined acted in good faith and without negligence.

Additionally, the bill provides that a person who files a fraudulent unclaimed funds report may be required by the Director to pay either or both of the following:

- \$500 per day, from the date the report is filed to the date the report is corrected, up to a maximum of \$25,000;
- 25% of the amount or value of any funds, property, or both, that was fraudulently reported.

The penalties for filing a fraudulent report are in addition to the penalties and interest described above for failing to timely report, pay, or deliver unclaimed funds.

Division of Liquor Control

Spirituos liquor sales

(R.C. 4301.19)

Current law allows the Division of Liquor Control to be the sole distributor and retail seller of spirituous liquor in Ohio. It distributes spirituous liquor through warehouses across Ohio and sells spirituous liquor at retail via agency stores. The bill clarifies that the Division also has authority to sell spirituous liquor from A-3a liquor permit premises (micro-distilleries, see below) because, under current law, those permit holders sell spirituous liquor that the permit holder manufactures under contract with the Division.

Liquor permit fees

D-7 liquor permit fee

(R.C. 4303.183)

Current law establishes the D-7 liquor permit fee (resort areas, see below) at \$469 per month for six months (length of the resort season). The bill stipulates that the fee is \$2,814 for the six months. There is no change in the fee since $\$469 \times 6 \text{ months} = \$2,814$.

F-4 liquor permit fee

(R.C. 4303.204)

For purposes of the current \$60 per-day fee required to obtain an F-4 liquor permit (Ohio wine festival, see below), which is issued for one to three days depending on the length of the festival, the bill does the following:

1. If the festival is one day, increases the fee from \$60 for the day to a flat fee of \$180;
2. If the festival is two days, increases the fee from \$120 for two days to a flat fee of \$180;
3. If the festival is three days, retains the \$180 fee.

F-11 liquor permit fee

(R.C. 4303.2011)

The bill makes similar changes to the F-11 liquor permit as it does for the F-4 permit described above. For purposes of the current \$60 per-day fee required to obtain an F-11 permit (Ohio craft beer festival, see below), which is issued for one to three days dependent on the length of the festival, the bill does the following:

1. If the festival is one day, increases the fee from \$60 for the day to a flat fee of \$180;
2. If the festival is two days, increases the fee from \$120 for two days to a flat fee of \$180;
3. If the festival is three days, retains the \$180 fee.

Under continuing law, the 3-day limitation does not apply to an exposition at the Ohio State Fairgrounds.

H liquor permit fee

(R.C. 4301.12 and 4301.30)

The bill transfers deposits of H liquor permit fees derived from permit holders whose permit premises are located outside Ohio from the existing Undivided Liquor Permit Fund to the existing State Liquor Regulatory Fund. Under current law, the Undivided Liquor Permit Fund is used for the following:

1. To fund alcohol treatment programs;
2. To fund local governments in which liquor permit premises are located; and
3. To be credited to the existing State Liquor Regulatory Fund, which is used to fund the Division of Liquor Control's operating expenses.

Under current law, the State Liquor Regulatory Fund consists of liquor permit fees from B-2a, S-1, and S-2 permits paid by B-2a, S-1, and S-2 permit holders that do not also hold A-1 or A-1c permits or A-2 or A-2f permits (see below).

S-2 liquor permit renewal fee

(R.C. 4303.233)

The bill increases from \$100 to \$250 the fee for the renewal of an S-2 liquor permit (large winery, see below), thus making the amount of the renewal fee equal to the \$250 fee for an initial S-2 liquor permit.

Background

Below is a list of permits referenced above, along with a description of the authorized activity under the permit.

Types of liquor permits	
Class of liquor permit	Authorized activity
A-1	Large brewery may sell its beer for on- or off-premises consumption.
A-1-A	Brewery, winery, or distillery may sell beer and any intoxicating liquor by glass or from a container; a brewery may sell beer for off-premises consumption.
A-1c	Craft brewery may sell its beer for on- or off-premises consumption.
A-2	Winery may sell wine to personal consumers for on- or off-premises consumption and to wholesalers.
A-2f	Farm winery (same authorized activity as a winery, but winery grows grapes and other agricultural products).
A-3a	Micro-distillery (less than 100,000 gallons a year) may sell to personal consumers a specified amount of spirituous liquor.
B-2a	Wine manufacturer may sell to retail liquor permit holders only wine it manufactures and for which a territory designation has not been filed with the state.
D-7	A restaurant or bar located in a resort area may sell beer or intoxicating liquor for on-premises consumption.
F-4	An Ohio wine festival organizer may give away 2 oz. samples of Ohio wine or sell individual glasses of wine for on-premises consumption and A-2 permit holder may sell bottles for off-premises consumption.
F-11	An Ohio craft beer festival organizer may sell 4 oz. samples or up to 16 oz. containers of craft beer for on-premises consumption.
H	Transporter or deliverer may transport or deliver beer and intoxicating liquor (not required for manufacturers or distributors).
S-1	Small brewery or small winery may sell their beer or wine directly to a personal consumer.

Types of liquor permits	
Class of liquor permit	Authorized activity
S-2	Large winery may sell their wine to a personal consumer either directly or through a fulfillment warehouse.