

As Passed by the House

132nd General Assembly

Regular Session

2017-2018

Sub. S. B. No. 220

Senators Hackett, Bacon

Cosponsors: Senators Coley, Burke, Dolan, Hoagland Representatives Anielski, Blessing, Brenner, Carfagna, Dean, Hambley, Lanese, Reineke, Riedel, Roegner, Seitz, Wiggam, Speaker Smith

A BILL

To amend sections 1306.01 and 3772.01 and to enact 1
sections 1354.01, 1354.02, 1354.03, 1354.04, and 2
1354.05 of the Revised Code to provide a legal 3
safe harbor to covered entities that implement a 4
specified cybersecurity program, to allow 5
transactions recorded by blockchain technology 6
under the Uniform Electronic Transactions Act, 7
and to alter the definition of "key employee" 8
under the Casino Gaming Law. 9

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF OHIO:

Section 1. That sections 1306.01 and 3772.01 be amended 10
and sections 1354.01, 1354.02, 1354.03, 1354.04, and 1354.05 of 11
the Revised Code be enacted to read as follows: 12

Sec. 1306.01. As used in sections 1306.01 to 1306.23 of 13
the Revised Code: 14

(A) "Agreement" means the bargain of the parties in fact, 15
as found in their language or inferred from other circumstances 16

and from rules, regulations, and procedures given the effect of 17
agreements under laws otherwise applicable to a particular 18
transaction. 19

(B) "Automated transaction" means a transaction conducted 20
or performed, in whole or in part, by electronic means or 21
electronic records, in which the acts or records of one or both 22
parties are not reviewed by an individual in the ordinary course 23
in forming a contract, performing under an existing contract, or 24
fulfilling an obligation required by the transaction. 25

(C) "Computer program" means a set of statements or 26
instructions to be used directly or indirectly in an information 27
processing system in order to bring about a certain result. 28

(D) "Contract" means the total legal obligation resulting 29
from the parties' agreement as affected by sections 1306.01 to 30
1306.23 of the Revised Code and other applicable law. 31

(E) "Electronic" means relating to technology having 32
electrical, digital, magnetic, wireless, optical, 33
electromagnetic, or similar capabilities. 34

(F) "Electronic agent" means a computer program or an 35
electronic or other automated means used independently to 36
initiate an action or respond to electronic records or 37
performances in whole or in part, without review or action by an 38
individual. 39

(G) "Electronic record" means a record created, generated, 40
sent, communicated, received, or stored by electronic means. A 41
record or contract that is secured through blockchain technology 42
is considered to be in an electronic form and to be an 43
electronic record. 44

(H) "Electronic signature" means an electronic sound, 45

symbol, or process attached to or logically associated with a 46
record and executed or adopted by a person with the intent to 47
sign the record. A signature that is secured through blockchain 48
technology is considered to be in an electronic form and to be 49
an electronic signature. 50

(I) "Governmental agency" means any executive, 51
legislative, or judicial agency, department, board, commission, 52
authority, institution, or instrumentality of the federal 53
government, of a state, or of a county, municipality, or other 54
political subdivision of a state. 55

(J) "Information" means data, text, images, sounds, codes, 56
computer programs, software, databases, or the like. 57

(K) "Information processing system" means an electronic 58
system for creating, generating, sending, receiving, storing, 59
displaying, or processing information. 60

(L) "Person" means an individual, corporation, business 61
trust, estate, trust, partnership, limited liability company, 62
association, joint venture, governmental agency, public 63
corporation, or any other legal or commercial entity. 64

(M) "Record" means information that is inscribed on a 65
tangible medium or that is stored in an electronic or other 66
medium and is retrievable in perceivable form. 67

(N) "Security procedure" means a procedure employed for 68
the purpose of verifying that an electronic signature, record, 69
or performance is that of a specific person or for detecting 70
changes or errors in the information in an electronic record. 71
"Security procedure" includes a procedure that requires the use 72
of algorithms or other codes, identifying word or numbers, 73
encryption, or callback or other acknowledgment procedures. 74

(O) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. "State" includes an Indian tribe or band, or Alaskan~~native~~ Native village, that is recognized by federal law or formally acknowledged by a state.

(P) "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Sec. 1354.01. As used in this chapter:

(A) "Business" means any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing.

(B) "Covered entity" means a business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state.

(C) "Data breach" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information owned by or licensed to a covered entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to person or property. "Data breach" does not include

either of the following: 104

(1) Good faith acquisition of personal information or 105
restricted information by the covered entity's employee or agent 106
for the purposes of the covered entity's, provided that the 107
personal information or restricted information is not used for 108
an unlawful purpose or subject to further unauthorized 109
disclosure; 110

(2) Acquisition of personal information or restricted 111
information pursuant to a search warrant, subpoena, or other 112
court order, or pursuant to a subpoena, order, or duty of a 113
regulatory state agency. 114

(D) "Personal information" has the same meaning as in 115
section 1349.19 of the Revised Code. 116

(E) "Restricted information" means any information about 117
an individual, other than personal information, that, alone or 118
in combination with other information, including personal 119
information, can be used to distinguish or trace the 120
individual's identity or that is linked or linkable to an 121
individual, if the information is not encrypted, redacted, or 122
altered by any method or technology in such a manner that the 123
information is unreadable, and the breach of which is likely to 124
result in a material risk of identity theft or other fraud to 125
person or property. 126

As used in this division, "encrypted," "individual," and 127
"redacted" have the same meanings as in section 1349.19 of the 128
Revised Code. 129

Sec. 1354.02. (A) A covered entity seeking an affirmative 130
defense under sections 1354.01 to 1354.05 of the Revised Code 131
shall do one of the following: 132

(1) Create, maintain, and comply with a written 133
cybersecurity program that contains administrative, technical, 134
and physical safeguards for the protection of personal 135
information and that reasonably conforms to an industry 136
recognized cybersecurity framework, as described in section 137
1354.03 of the Revised Code; or 138

(2) Create, maintain, and comply with a written 139
cybersecurity program that contains administrative, technical, 140
and physical safeguards for the protection of both personal 141
information and restricted information and that reasonably 142
conforms to an industry recognized cybersecurity framework, as 143
described in section 1354.03 of the Revised Code. 144

(B) A covered entity's cybersecurity program shall be 145
designed to do all of the following with respect to the 146
information described in division (A) (1) or (2) of this section, 147
as applicable: 148

(1) Protect the security and confidentiality of the 149
information; 150

(2) Protect against any anticipated threats or hazards to 151
the security or integrity of the information; 152

(3) Protect against unauthorized access to and acquisition 153
of the information that is likely to result in a material risk 154
of identity theft or other fraud to the individual to whom the 155
information relates. 156

(C) The scale and scope of a covered entity's 157
cybersecurity program under division (A) (1) or (2) of this 158
section, as applicable, is appropriate if it is based on all of 159
the following factors: 160

(1) The size and complexity of the covered entity; 161

<u>(2) The nature and scope of the activities of the covered</u>	162
<u>entity;</u>	163
<u>(3) The sensitivity of the information to be protected;</u>	164
<u>(4) The cost and availability of tools to improve</u>	165
<u>information security and reduce vulnerabilities;</u>	166
<u>(5) The resources available to the covered entity.</u>	167
<u>(D) (1) A covered entity that satisfies divisions (A) (1),</u>	168
<u>(B), and (C) of this section is entitled to an affirmative</u>	169
<u>defense to any cause of action sounding in tort that is brought</u>	170
<u>under the laws of this state or in the courts of this state and</u>	171
<u>that alleges that the failure to implement reasonable</u>	172
<u>information security controls resulted in a data breach</u>	173
<u>concerning personal information.</u>	174
<u>(2) A covered entity that satisfies divisions (A) (2), (B),</u>	175
<u>and (C) of this section is entitled to an affirmative defense to</u>	176
<u>any cause of action sounding in tort that is brought under the</u>	177
<u>laws of this state or in the courts of this state and that</u>	178
<u>alleges that the failure to implement reasonable information</u>	179
<u>security controls resulted in a data breach concerning personal</u>	180
<u>information or restricted information.</u>	181
<u>Sec. 1354.03. A covered entity's cybersecurity program, as</u>	182
<u>described in section 1354.02 of the Revised Code, reasonably</u>	183
<u>conforms to an industry recognized cybersecurity framework for</u>	184
<u>purposes of that section if division (A), (B), or (C) of this</u>	185
<u>section is satisfied.</u>	186
<u>(A) (1) The cybersecurity program reasonably conforms to</u>	187
<u>the current version of any of the following or any combination</u>	188
<u>of the following, subject to divisions (A) (2) and (D) of this</u>	189
<u>section:</u>	190

<u>(a) The "framework for improving critical infrastructure</u>	191
<u>cybersecurity" developed by the "national institute of standards</u>	192
<u>and technology" (NIST);</u>	193
<u>(b) "NIST special publication 800-171";</u>	194
<u>(c) "NIST special publications 800-53 and 800-53a";</u>	195
<u>(d) The "federal risk and authorization management program</u>	196
<u>(FedRAMP) security assessment framework";</u>	197
<u>(e) The "center for internet security critical security</u>	198
<u>controls for effective cyber defense";</u>	199
<u>(f) The "international organization for</u>	200
<u>standardization/international electrotechnical commission 27000</u>	201
<u>family - information security management systems."</u>	202
<u>(2) When a final revision to a framework listed in</u>	203
<u>division (A) (1) of this section is published, a covered entity</u>	204
<u>whose cybersecurity program reasonably conforms to that</u>	205
<u>framework shall reasonably conform to the revised framework not</u>	206
<u>later than one year after the publication date stated in the</u>	207
<u>revision.</u>	208
<u>(B) (1) The covered entity is regulated by the state, by</u>	209
<u>the federal government, or both, or is otherwise subject to the</u>	210
<u>requirements of any of the laws or regulations listed below, and</u>	211
<u>the cybersecurity program reasonably conforms to the entirety of</u>	212
<u>the current version of any of the following, subject to division</u>	213
<u>(B) (2) of this section:</u>	214
<u>(a) The security requirements of the "Health Insurance</u>	215
<u>Portability and Accountability Act of 1996," as set forth in 45</u>	216
<u>CFR Part 164 Subpart C;</u>	217
<u>(b) Title V of the "Gramm-Leach-Bliley Act of 1999,"</u>	218

<u>Public Law 106-102, as amended;</u>	219
<u>(c) The "Federal Information Security Modernization Act of 2014," Public Law 113-283;</u>	220
<u>(d) The "Health Information Technology for Economic and Clinical Health Act," as set forth in 45 CFR part 162.</u>	222
<u>(2) When a framework listed in division (B)(1) of this section is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the amended framework not later than one year after the effective date of the amended framework.</u>	224
<u>(C)(1) The cybersecurity program reasonably complies with both the current version of the "payment card industry (PCI) data security standard" and conforms to the current version of another applicable industry recognized cybersecurity framework listed in division (A) of this section, subject to divisions (C)(2) and (D) of this section.</u>	229
<u>(2) When a final revision to the "PCI data security standard" is published, a covered entity whose cybersecurity program reasonably complies with that standard shall reasonably comply with the revised standard not later than one year after the publication date stated in the revision.</u>	230
<u>(D) If a covered entity's cybersecurity program reasonably conforms to a combination of industry recognized cybersecurity frameworks, or complies with a standard, as in the case of the payment card industry (PCI) data security standard, as described in division (A) or (C) of this section, and two or more of those frameworks are revised, the covered entity whose cybersecurity program reasonably conforms to or complies with, as applicable, those frameworks shall reasonably conform to or comply with, as</u>	231
	232
	233
	234
	235
	236
	237
	238
	239
	240
	241
	242
	243
	244
	245
	246
	247

applicable, all of the revised frameworks not later than one 248
year after the latest publication date stated in the revisions. 249

Sec. 1354.04. Sections 1354.01 to 1354.05 of the Revised 250
Code shall not be construed to provide a private right of 251
action, including a class action, with respect to any act or 252
practice regulated under those sections. 253

Sec. 1354.05. If any provision of sections 1354.01 to 254
1354.05 of the Revised Code or the application thereof to a 255
covered entity is for any reason held to be invalid, the 256
remainder of the provisions under those sections and the 257
application of such provisions to other covered entities shall 258
not be thereby affected. 259

Sec. 3772.01. As used in this chapter: 260

(A) "Applicant" means any person who applies to the 261
commission for a license under this chapter. 262

(B) "Casino control commission fund" means the casino 263
control commission fund described in Section 6(C) (3) (d) of 264
Article XV, Ohio Constitution, the money in which shall be used 265
to fund the commission and its related affairs. 266

(C) "Casino facility" means a casino facility as defined 267
in Section 6(C) (9) of Article XV, Ohio Constitution. 268

(D) "Casino game" means any slot machine or table game as 269
defined in this chapter. 270

(E) "Casino gaming" means any type of slot machine or 271
table game wagering, using money, casino credit, or any 272
representative of value, authorized in any of the states of 273
Indiana, Michigan, Pennsylvania, and West Virginia as of January 274
1, 2009, and includes slot machine and table game wagering 275

subsequently authorized by, but shall not be limited by, 276
subsequent restrictions placed on such wagering in such states. 277
"Casino gaming" does not include bingo, as authorized in Section 278
6 of Article XV, Ohio Constitution and conducted as of January 279
1, 2009, or horse racing where the pari-mutuel system of 280
wagering is conducted, as authorized under the laws of this 281
state as of January 1, 2009. 282

(F) "Casino gaming employee" means any employee of a 283
casino operator or management company, but not a key employee, 284
and as further defined in section 3772.131 of the Revised Code. 285

(G) "Casino operator" means any person, trust, 286
corporation, partnership, limited partnership, association, 287
limited liability company, or other business enterprise that 288
directly or indirectly holds an ownership or leasehold interest 289
in a casino facility. "Casino operator" does not include an 290
agency of the state, any political subdivision of the state, any 291
person, trust, corporation, partnership, limited partnership, 292
association, limited liability company, or other business 293
enterprise that may have an interest in a casino facility, but 294
who is legally or contractually restricted from conducting 295
casino gaming. 296

(H) "Central system" means a computer system that provides 297
the following functions related to casino gaming equipment used 298
in connection with casino gaming authorized under this chapter: 299
security, auditing, data and information retrieval, and other 300
purposes deemed necessary and authorized by the commission. 301

(I) "Cheat" means to alter the result of a casino game, 302
the element of chance, the operation of a machine used in a 303
casino game, or the method of selection of criteria that 304
determines (a) the result of the casino game, (b) the amount or 305

frequency of payment in a casino game, (c) the value of a 306
wagering instrument, or (d) the value of a wagering credit. 307
"Cheat" does not include an individual who, without the 308
assistance of another individual or without the use of a 309
physical aid or device of any kind, uses the individual's own 310
ability to keep track of the value of cards played and uses 311
predictions formed as a result of the tracking information in 312
the individual's playing and betting strategy. 313

(J) "Commission" means the Ohio casino control commission. 314

(K) "Gaming agent" means a peace officer employed by the 315
commission that is vested with duties to enforce this chapter 316
and conduct other investigations into the conduct of the casino 317
gaming and the maintenance of the equipment that the commission 318
considers necessary and proper and is in compliance with section 319
109.77 of the Revised Code. 320

(L) "Gaming-related vendor" means any individual, 321
partnership, corporation, association, trust, or any other group 322
of individuals, however organized, who supplies gaming-related 323
equipment, goods, or services to a casino operator or management 324
company, that are directly related to or affect casino gaming 325
authorized under this chapter, including, but not limited to, 326
the manufacture, sale, distribution, or repair of slot machines 327
and table game equipment. 328

(M) "Holding company" means any corporation, firm, 329
partnership, limited partnership, limited liability company, 330
trust, or other form of business organization not a natural 331
person which directly or indirectly does any of the following: 332

(1) Has the power or right to control a casino operator, 333
management company, or gaming-related vendor license applicant 334

or licensee; 335

(2) Holds an ownership interest of five per cent or more, 336
as determined by the commission, in a casino operator, 337
management company, or gaming-related vendor license applicant 338
or licensee; 339

(3) Holds voting rights with the power to vote five per 340
cent or more of the outstanding voting rights of a casino 341
operator, management company, or gaming-related vendor applicant 342
or licensee. 343

(N) "Initial investment" includes costs related to 344
demolition, engineering, architecture, design, site preparation, 345
construction, infrastructure improvements, land acquisition, 346
fixtures and equipment, insurance related to construction, and 347
leasehold improvements. 348

(O) "Institutional investor" means any of the following 349
entities owning five per cent or more, but less than fifteen per 350
cent, of an ownership interest in a casino facility, casino 351
operator, management company, or holding company: a corporation, 352
bank, insurance company, pension fund or pension fund trust, 353
retirement fund, including funds administered by a public 354
agency, employees' profit-sharing fund or employees' profit- 355
sharing trust, any association engaged, as a substantial part of 356
its business or operations, in purchasing or holding securities, 357
including a hedge fund, mutual fund, or private equity fund, or 358
any trust in respect of which a bank is trustee or cotrustee, 359
investment company registered under the "Investment Company Act 360
of 1940," 15 U.S.C. 80a-1 et seq., collective investment trust 361
organized by banks under Part Nine of the Rules of the 362
Comptroller of the Currency, closed-end investment trust, 363
chartered or licensed life insurance company or property and 364

casualty insurance company, investment advisor registered under 365
the "Investment Advisors Act of 1940," 15 U.S.C. 80 b-1 et seq., 366
and such other persons as the commission may reasonably 367
determine to qualify as an institutional investor for reasons 368
consistent with this chapter, and that does not exercise control 369
over the affairs of a licensee and its ownership interest in a 370
licensee is for investment purposes only, as set forth in 371
division (E) of section 3772.10 of the Revised Code. 372

(P) "Key employee" means any executive, employee, ~~or~~ 373
agent, or other individual who has the power to exercise 374
significant influence over decisions concerning any part of the 375
operation of a person that has applied for or holds a casino 376
operator ~~or~~, management company licensee having the power to 377
exercise significant influence over decisions concerning any 378
part of the operation of such licensee, or gaming-related vendor 379
license or the operation of a holding company of a person that 380
has applied for or holds a casino operator, management company, 381
or gaming-related vendor license, including: 382

(1) ~~An officer, director, trustee, or partner of a person~~ 383
~~that has applied for or holds a casino operator, management~~ 384
~~company, or gaming-related vendor license or of a holding~~ 385
~~company that has control of a person that has applied for or~~ 386
~~holds a casino operator, management company, or gaming related~~ 387
~~vendor license, or an equivalent fiduciary;~~ 388

(2) ~~A person that~~ An individual who holds a direct or 389
indirect ownership interest of ~~more than one~~ five per cent ~~in a~~ 390
~~person that has applied for or holds a casino operator,~~ 391
~~management company, or gaming-related vendor license or holding~~ 392
~~company that has control of a person that has applied for or~~ 393
~~holds a casino operator, management company, or gaming related~~ 394

~~vendor license or more;~~ 395

~~(3) A managerial employee of a person that has applied for or holds a casino operator or gaming-related vendor license in Ohio, or a managerial employee of a holding company that has control of a person that has applied for or holds a casino operator or gaming-related vendor license in Ohio, An individual who performs the function of a principal executive officer, principal operating officer, principal accounting officer, or an equivalent officer or;~~ 396
397
398
399
400
401
402
403

~~(4) Any other person individual the commission determines to have the power to exercise significant influence over decisions concerning any part of the operation of such licensee.~~ 404
405
406

~~The commission shall determine whether an individual whose duties or status varies from those described in this division also is considered a key employee.~~ 407
408
409

(Q) "Licensed casino operator" means a casino operator that has been issued a license by the commission and that has been certified annually by the commission to have paid all applicable fees, taxes, and debts to the state. 410
411
412
413

(R) "Majority ownership interest" in a license or in a casino facility, as the case may be, means ownership of more than fifty per cent of such license or casino facility, as the case may be. For purposes of the foregoing, whether a majority ownership interest is held in a license or in a casino facility, as the case may be, shall be determined under the rules for constructive ownership of stock provided in Treas. Reg. 1.409A-3(i)(5)(iii) as in effect on January 1, 2009. 414
415
416
417
418
419
420
421

(S) "Management company" means an organization retained by a casino operator to manage a casino facility and provide 422
423

services such as accounting, general administration, 424
maintenance, recruitment, and other operational services. 425

(T) "Ohio law enforcement training fund" means the state 426
law enforcement training fund described in Section 6(C) (3) (f) of 427
Article XV, Ohio Constitution, the money in which shall be used 428
to enhance public safety by providing additional training 429
opportunities to the law enforcement community. 430

(U) "Person" includes, but is not limited to, an 431
individual or a combination of individuals; a sole 432
proprietorship, a firm, a company, a joint venture, a 433
partnership of any type, a joint-stock company, a corporation of 434
any type, a corporate subsidiary of any type, a limited 435
liability company, a business trust, or any other business 436
entity or organization; an assignee; a receiver; a trustee in 437
bankruptcy; an unincorporated association, club, society, or 438
other unincorporated entity or organization; entities that are 439
disregarded for federal income tax purposes; and any other 440
nongovernmental, artificial, legal entity that is capable of 441
engaging in business. 442

(V) "Problem casino gambling and addictions fund" means 443
the state problem gambling and addictions fund described in 444
Section 6(C) (3) (g) of Article XV, Ohio Constitution, the money 445
in which shall be used for treatment of problem gambling and 446
substance abuse, and for related research. 447

(W) "Promotional gaming credit" means a slot machine or 448
table game credit, discount, or other similar item issued to a 449
patron to enable the placement of, or increase in, a wager at a 450
slot machine or table game. 451

(X) "Slot machine" means any mechanical, electrical, or 452

other device or machine which, upon insertion of a coin, token, 453
ticket, or similar object, or upon payment of any consideration, 454
is available to play or operate, the play or operation of which, 455
whether by reason of the skill of the operator or application of 456
the element of chance, or both, makes individual prize 457
determinations for individual participants in cash, premiums, 458
merchandise, tokens, or any thing of value, whether the payoff 459
is made automatically from the machine or in any other manner, 460
but does not include any device that is a skill-based amusement 461
machine, as defined in section 2915.01 of the Revised Code. 462

(Y) "Table game" means any game played with cards, dice, 463
or any mechanical, electromechanical, or electronic device or 464
machine for money, casino credit, or any representative of 465
value. "Table game" does not include slot machines. 466

(Z) "Upfront license" means the first plenary license 467
issued to a casino operator. 468

(AA) "Voluntary exclusion program" means a program 469
provided by the commission that allows persons to voluntarily 470
exclude themselves from the gaming areas of facilities under the 471
jurisdiction of the commission by placing their name on a 472
voluntary exclusion list and following the procedures set forth 473
by the commission. 474

Section 2. That existing sections 1306.01 and 3772.01 of 475
the Revised Code are hereby repealed. 476

Section 3. (A) The purpose of this act is to establish a 477
legal safe harbor to be pled as an affirmative defense to a 478
cause of action sounding in tort that alleges or relates to the 479
failure to implement reasonable information security controls, 480
resulting in a data breach. The safe harbor shall apply to all 481

covered entities that implement a cybersecurity program that 482
meets the requirements of the act. 483

(B) This act is intended to be an incentive and to 484
encourage businesses to achieve a higher level of cybersecurity 485
through voluntary action. The act does not, and is not intended 486
to, create a minimum cybersecurity standard that must be 487
achieved, nor shall it be read to impose liability upon 488
businesses that do not obtain or maintain practices in 489
compliance with the act. 490