Introduction

This submission discusses two Illinois statutes, 1) Illinois’ law regarding the use of CBD oil in products to be sold to the public, as well as 2) Illinois’ law relating to protecting the privacy of personal information of consumers.

Illinois’ laws related to the use of CBD oil in products to be sold to the public run on two parallel tracks defined by which version of the cannabis sativa plant the CBD is derived from. The first being products containing CBD derived from hemp, and the second being products containing CBD derived from marijuana. The difference being that the public may purchase hemp CBD products (less than 0.3% THC) over-the-counter without any restrictive licensing or registration, whereas the purchase of CBD products from marijuana (unrestricted levels of THC) currently requires the purchaser to hold a medical cannabis registration card and must be purchased from a licensed dispensary under Illinois’ Compassionate Use of Medical Cannabis program, enacted in 2014.

However, in May of 2019, Illinois passed legislation known as the Cannabis Regulation and Tax Act (CRTA), which upon Gov. J.B. Pritzker’s anticipated signing, will make adult sales and use of recreational marijuana legal throughout the state. IL HB 1438. When the CRTA goes into effect on January 1, 2020, the public in Illinois will be able to purchase recreational and medical marijuana, including CBD products (with varying levels of THC), legally at licensed dispensaries, without the need for any registration such as is required under the current medical cannabis program. For purposes of discussing Illinois’ law specifically related to the sale of CBD products to the public, only the Illinois Industrial Hemp Act is discussed herein; however, a summary of Illinois’ Cannabis Regulation and Tax Act is attached hereto.

By placing a number of requirements on companies and other organizations that handle, collect, disseminate, or otherwise deal with nonpublic personal information, the Illinois Personal Information Protection Act, 815 ILCS 530, et seq., is one of the most stringent data breach laws in the country. The relevant provisions as amended are summarized herein, and a copy of the statute is attached hereto for reference.
1. What is your state’s law on the use of CBD oil in products to be sold to the public, i.e. cosmetics, etc.?

Illinois was a major producer of hemp until it was criminalized in 1937. In 2014, Congress reopened the market when it passed the 2014 Farm Bill. The Farm Bill authorized states to launch research pilot projects. In 2018, the hemp production became fully legal under Federal law with passage of the 2018 Farm Bill which allowed States to authorize hemp production of plants containing no more than 0.3% THC, the psychoactive chemical in marijuana.

Illinois authorized hemp production in August, 2018 upon passage of the State’s Industrial Hemp Act. 505 ILCS 89. Illinois’ Industrial Hemp Act (the Act) established a legal framework allowing Illinois to grow, cultivate, process and sell industrial hemp and related products subject the Illinois’ Department of Agriculture’s (IDOA’s) rules. The Act also amended both the State’s Noxious Weed Act, 505 ILCS 100/2, and Cannabis Control Act 720 ILCS 550/3, removing hemp from both legal categories as recognized by State law, respectfully. 505 ILCS 89/900 and 89/905

The Act defines industrial hemp as, “the plant Cannabis sativa L. and any part of that plant, whether growing or not, with a delta-9 tetrahydrocannabinol concentration (THC) of not more than 0.3 % on a dry weight basis that has been cultivated under a license issued under this Act or is otherwise lawfully present in this State, and includes any intermediate or finished product made or derived from industrial hemp.” 505 ILCS 89/5. The definition includes all CBD products to be sold to the public, including not only topicals, creams and cosmetics, but also foods, beverages and health supplements. There are no restrictions within the Act that excludes the production and sale of CBD products in foods, beverages or health supplement products. However, the Act further provides that Federal law preempts the Act in situations of conflict. CBD products will be limited to the provisions and rules the USDA is anticipated to publish relating to CBD in foods, beverages and health supplements pursuant to the 2018 Farm Bill. 505 ILCS 89/25 Further, the Act does not alter the legality of hemp or hemp products that are presently legal to possess or own. 505 ILCS 89/20

Licensing is only required for cultivation of industrial hemp and not for processing, transportation or sales of hemp products such as those containing CBD. 505 ILCS 89/10 However, handling and processing raw industrial hemp into another form or product requires
registration with the IDOA. Id. There is no licensing or registration requirements in the Act related to the sale of CBD products to the public. The Act requires all hemp crops to be tested for THC content a minimum of once per year with the possibility of “additional unannounced inspections” 505 ILCS 89/15

The IDOA has published its rules applicable to the program. It should be noted that Section 1200.90 (c) of the IDOA Adopted Rules dealing with Restrictions on Sale and Transfer provides “[T]he Department shall permit the sale or transfer of stripped stalks, fiber, dried roots, nonviable seeds, seed oils, floral and plant extracts (excluding THC in excess of 0.3%) and other marketable hemp products to members of the general public, both within and outside the State of Illinois,” thereby allowing for the sale of products containing CBD to the public.

2. Regarding privacy issues, has your state adopted its own version of GDPR or how is your state dealing with GDPR requirements? What other privacy laws has your state adopted recently in response to concerns about the lack of protections for consumers?

The Illinois Personal Information Act (PIPA), 815 ILCS § 530, originally enacted in 2005 applies to any entity that handles, collects, disseminates, or otherwise deals with nonpublic personal information. PIPA imposes certain obligations on these entities in the event of a breach of Illinois residents’ personal information. On January 1, 2017, PIPA broadened and strengthened its personal information and data breach regime with several new provisions.

The definition of personal information was expanded in a couple ways. First, the definition as tied to a person’s name and other identifying information was expanded to mean a person’s first name or initial and their last name along with other identifying details such as a Social Security number, when such information is not encrypted or redacted or when the access to the shielded information has been hacked. In addition, the list of identifying details was expanded to include medical information, health insurance information and unique biometric data such as fingerprints. Health insurance information is defined as an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual’s health insurance application and claims history, including any appeals records. Medical information is defined as any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to websites or mobile applications. Second, a new definition of personal information was added to include a person’s user name or email address, in combination with a password or security question and answer, that would permit access to an online account, when such information is not encrypted, redacted or when access to the shielded information has been hacked. 815 ILCS § 530/5

The PIPA statute is triggered upon discovery or notification of a breach of security of the system. “Breach of security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. Data collectors or service providers who maintain or store, but do not own or license personal information, must
cooperate with the data owner or licensor with respect to breaches of personal information in the service provider’s care. The cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector’s cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach. PIPA’s requirement for issuing a notice of breach has been amended to address the new online account definition of personal information. When the breach concerns this type of personal information, notice may be provided in electronic or other form and must direct the Illinois resident to promptly change the information that has been breached for the resident’s account identified by the entity providing notice and all other accounts for which the resident uses the same user name, password or security question and answer. 815 ILCS § 530/10

Notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system. If a law enforcement agency determines that providing notice will interfere with a written request to delay notification, the data collector may delay notice until notification will no longer interfere with a criminal investigation. 815 ILCS 530/10 (a)

The PIPA statute extends the data security requirements to any entity covered by the Act that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident. Under the amended Act, such an entity shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS § 530/45(a) In addition, if an entity has a contract for the disclosure of such information, it must specify that the person obtaining the information must also maintain such security measures. 815 ILCS § 530/45(b) The Act confirms that an entity’s compliance with an applicable state or federal law (including the Gramm-Leach-Bliley Act of 1999) calling for “greater protection” constitutes compliance with the Act. 815 ILCS § 530/45(c) and (d) As to entities subject to the federal Health Insurance Portability and Accountability Act of 1995 and the Health Information Technology for Economic and Clinical Health Act, the Act provides that compliance with those federal laws is sufficient so long as notification of a breach is made to the Secretary of Health and Human Services and to the State’s Attorney General within five business days thereafter. 815 ILCS § 530/50

Violations constitute an unlawful practice under the Illinois’ Consumer Fraud and Deceptive Business Practices Act and any person who suffers actual damages may bring an action under the statute. Violations are subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation. A civil penalty may not exceed $50,000 for each instance of improper disposal. The Attorney General may impose a civil penalty after issuing notice to the person accused of violating this section. In addition, the Attorney General is empowered to bring an action in the circuit court to remedy a violation and seek appropriate relief. 815 ILCS 530/20
Recently, on May 27, 2019, the Illinois General Assembly approved Senate Bill 1624, an amendment to PIPA, which is expected to be signed by Illinois Governor J.B. Pritzker in short order. In the amendment, Section 10 of PIPA would strengthen the obligations of data collectors requiring them to also notify the Office of the Attorney General of any breach affecting more than 500 Illinois residents. Under the amendment, data collectors must provide the Attorney General with a description of the breach, the number of affected residents and details of any steps taken related to the incident. The amendment grants the Attorney General authority to publish the name of the data collector, the types of personal information compromised and other relevant information that will further ensure that residents are notified of the breach in a timely manner.