PRIVACY AND DATA SECURITY ISSUES FACING CITIES

TEXAS CITY ATTORNEYS ASSOCIATION
2016 Summer Conference
Hyatt Regency Lost Pines Resort and Spa
June 15-17, 2016
Bastrop, Texas

LISA D. MARES
Brown & Hofmeister, L.L.P.
740 East Campbell, Suite 800
Richardson, Texas 75081
(214) 747-6100 ✯ www.bhlaw.net

Lisa D. Mares

Lisa graduated from The University of Texas at Austin with a Bachelor of Arts in Sociology, obtained her Master of Public Policy degree from Duke University's Sanford School, and earned a law degree from the University of North Carolina at Chapel Hill. Lisa has served the public in various capacities, including an Elections Coordinator for the Travis County Clerk's Office and an Assistant Committee Clerk for the House Committee on Criminal Jurisprudence of the Texas State Legislature. During the joint degree program, she was a policy intern for the North Carolina Department of Juvenile Justice and Delinquency Prevention and the Mexican-American Legal Defense and Educational Fund, as well as a law clerk for the North Carolina Department of Justice, the North Carolina State Board of Elections, and the Charlotte City Attorney's Office.

Lisa has nine years of experience representing cities, political subdivisions, special districts, non-profit organizations, state agencies, a regional tollway authority in all aspects of government law and board governance, including administrative law, election law, employment law, conflicts of interest, intellectual property, land use, legislative advocacy, policy development, procurement, regulatory compliance, open government, and criminal prosecution. Lisa's previous work experience includes legislative analysis and developing and implementing statewide policy initiatives. Lisa currently practices municipal law as an Associate with Brown & Hofmeister in Richardson, Texas.

TABLE OF CONTENTS

APPENDIX

I. INTRODUCTION

Federal, state and local governments hold a wide variety of data about businesses and individuals.[1] The types of data held by public entities range from intellectual property and trade secrets found in bidding documents to financial information submitted in tax and business records. Public entities also maintain an abundance - in amount and assortment - of personal information. For instance, public entities maintain sensitive health information found in employment and ambulatory medical records to personal criminal history record information from police records, to motor vehicle information acquired by traffic citations.[2] Public entities acquire data in various ways, such as while carrying out governmental functions for law enforcement or fire prevention purposes. Individuals also supply personal information to public entities as job applicants, employees or to obtain a government benefit. Furthermore, private entities share information with public entities pursuant to regulatory disclosures, the procurement process, or data sharing agreements.[3]

Some legal scholars argue that a public entity has a "heightened" duty to safeguard business and personal information that is acquires.[4] This paper discusses a city's legal obligations to protect the personally identifiable information it acquires from unauthorized access or disclosure, as well as ensure that such information is accurate, and is intended to be a resource for city attorneys and outside counsel who advise cities how to safeguard the integrity, confidentiality and storage of personal data. To that end, this paper is organized as follows: Part II discusses data acquired by public entities; Part III of this paper briefly discusses direct and indirect costs of a data breach; Part IV provides an overview of state laws regulating sensitive personal information and protected health information held by public entities, select federal laws that regulate the disclosure of individually identifiable information, and industry standards the regulate the collection of information in connection with credit card transactions; Part V addresses barriers to establishing standing in data privacy litigation, efforts to establish standing solely via a statutory violation, and recent class actions litigation against the federal government due to a massive data breach; and the Appendix includes resources on data privacy.

II. BREACH OF PUBLIC DATA

Records and data held by public entities ("public data") are at risk for breach. In general, a "breach" is defined as "an event in which an individual's name plus social security number, medical record, and/or financial information is at risk due to accidental or deliberate unauthorized disclosure."[5] There is a multitude of ways that sensitive data can be disclosed without authorization. Data is unintentionally disclosed when records, portable devices, or

---

[1] A. Michael Froomkin, *Government Data Breaches*, 24 BERKELEY TECH L.J. 1019, 1022 (2009).

[2] *See id.*; Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 439 (2009); U.S. GEN. ACCOUNTING OFFICE, GAO-04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 3 (2004) [hereinafter, GAO, DATA MINING]; Paul Lipman, *4 Critical Challenges to State and Local Government Cybersecurity Efforts* (Industry Perspective), GOVERNMENT TECHNOLOGY, ¶ 4 (2015), http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html.

[3] *See* Froomkin, *supra* note 1, at 1019, 1022; Cate, *supra* note 2; *see also* GAO, DATA MINING, *supra* note 2.

[4] *See* Froomkin, *supra* note 1.

[5] Ponemon Institute, *2015 Costs of Data Breach Study: United States* 4 (2015) [hereinafter Ponemon, *Costs of Data Breach*].

computers are lost or improperly discarded, or when an individual inadvertently emails records to the wrong person or posts records on a website.[6] Data can also be deliberately accessed without authorization via theft, fraud or hacking.[7] As observed by Paul Lipman, CEO of iSheriff, "[t]he massive amount of valuable data housed by state and local agencies is an attractive target for cybercriminals seeking financial gain."[8] Yet, when compared to the cybersecurity efforts of 17 other major industries, public entities ranked at the bottom of major industries, ranking below information services, financial services, transportation, and healthcare.[9]

Data that is deliberately accessed without authorization may not necessarily be used for financial gain. There has been an increase in using targeted cyber attacks in the form of cyber espionage or hacktivism. Cyber espionage is used by "digital intelligence agents co-opt surveillance systems, track government employees, and exfiltrate documents for strategic advantage."[10] Cyber espionage is a tool that is usually used by, or on behalf of, government actors.[11] Of the organizations that have experienced a cyber espionage incident impacting the confidentiality, integrity or availability of its data, organizations that fall within the public sector are most targeted.[12] Likened to protests or civil disobedience, the term "hacktivism" refers to computer hacking for a political purpose or to influence action or a social cause, such as free speech, human rights or information access.[13] Techniques used by so-called hacktivists include defacing or parodying websites, redirecting URLs, denial-of-service attacks, stealing information, virtual sit-ins, and virtual sabotage.[14] These types of attacks can result in a great deal of economic harm to an individual, a business, and can even threaten critical infrastructure.[15]

III. COSTS OF DATA BREACH

Whether public or private, an entity faces significant costs when responding to a breach incident. The expenses faced by an entity include the costs to detect, recover, investigate, and manage incident response. Additional expenses incurred by the breached entity include indirect costs to mitigate financial loss faced by customers and minimize disruptions to operations.[16] For

---

[6] Privacy Rights Clearinghouse, *Chronology of Data Breaches* (2016), http://www.privacyrights.org/data-breach/new [hereinafter Privacy Rights, *Chronology of Data Breaches*].
[7] *Id.*; Ponemon, *Costs of Data Breach*, *supra* note 5, at 8.
[8] Lipman, *supra* note 4, at ¶ 4.
[9] SecurityScorecard R&D Department, *2016 U.S. Government Cybersecurity Report* 3 (2016), http://info.securityscorecard.com/2016-us-government-cybersecurity-report.
[10] McAfee Labs, *2016 Threats Predictions* 17, 35 (2015), http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf.
[11] OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009-2011 1, A-1, B-1 thru B-3 (2011).
[12] Verizon Enterprises, *2016 Data Breach Investigations Report* (2016), http://www.verizonenterprise.com/verizon-insights-lab/dbir/.
[13] McAfee Labs, *supra* note 10.
[14] Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation 3, 6, 104, 124 (September 2004) (unpublished Ph.D. thesis, Harvard University) (*available at* http://alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf).
[15] Verizon Enterprises, *supra* note 12, at 80.
[16] Ponemon Institute, *2015 Costs of Cyber Crime Study: United States* 1 (2015).

public or private entities located in the United States, the cost of a single data breach incident is estimated at $6.5 million or an average of $217 per individual record that was lost or stolen.[17] The public sector has the lowest average cost of a data breach per individual record when compared to other industries. For instance, the average cost of a data breach per record is $73 for the public sector, compared to $398 per record for the healthcare industry.[18] These figures beg the question, "*why the difference?*" The answer stems, in part, from the types of services offered by the public and private sector. Much of the personal or business information that a public entity collects is acquired pursuant to a legal requirement, in connection with a government benefit, or due to a licensing condition or regulatory compliance.[19] The health, financial, technology, and service industries likely experience higher indirect costs due to a loss in customers, while the public sector experiences lower indirect costs due to customer loss because government benefit recipients and regulated entities are parties to an involuntary transaction, and have few or no alternatives to dealing with the breached public entity.[20]

The answer to the inquiry regarding why a breached public entity faces lower costs than a breached private entity also stems from how state and federal governments self-regulate with respect to the data that governments create, collect and access.[21] Many state and federal laws exempt public data breaches from civil and criminal penalties. Even when a public entity is subject to penalties, they are only imposed if the public entity's conduct is egregious. One of the first public entities to enter into a settlement agreement due to a violation of the Health Insurance Portability and Accountability Act ("HIPAA") violation is Skagit County, Washington in 2014.

The Skagit County health department improperly posted the medical payment records of 1,600 patients on a public web server. The records contained patient first and last names, the health service received, medical procedure and diagnostic codes, the date of payment, and in cases where a patient paid with a credit or debit card, the last 4 digits of the card.[22] Additional violations noted by the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") included non-compliance with the Breach Notification Rule and the Security Rule by failing to notify affected persons of the breach, to maintain security policy and procedures, and to train personnel to maintain the privacy and security of protected health information.[23] The County entered into a settlement agreement of $215,000 and a corrective action plan with the OCR. OCR noted that "[t]his case marks the first settlement with a county government and sends a strong message about the importance of HIPAA compliance to local and county governments, regardless of size."[24] The OCR indicated that state and local governments are not immune from

---

[17] Ponemon, *Costs of Data Breach*, *supra* note 5, at 1.
[18] *Id*. at 7.
[19] Froomkin, *supra* note 1, at 1019, 1023-25.
[20] Ponemon, *Costs of Data Breach*, *supra* note 5, at 11; Froomkin, *supra* note 1, at 1019, 1025.
[21] Cate, *supra* note 2, at fn. 7, 435, 437-38.
[22] Skagit County, Washington, Notice of HIPAA Breach (*available at* http://www.skagitcounty.net/Departments/Home/hipaa.htm).
[23] U.S. Dep't of Health & Human Services, Resolution Agreement and Corrective Action Plan with Skagit County, Washington 1-2 (March 6, 2014) (*available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/skagit-county-settlement-agreement.pdf).
[24] Press Release, U.S. Dep't of Health & Human Services, County Government Settles Potential HIPAA Violations, ¶ 2 (March 7, 2014) (*available at* http://www.hhs.gov/about/news/2014/03/07/county-government-settles-potential-hipaa-violations.html).

future enforcement actions and that such "agencies need to adopt a meaningful compliance program to ensure the privacy and security of patients' information."[25]

Despite warnings of the necessity to secure individually identifiable data, more than 177 million records held by public entities are estimated to have been lost or breached since 2006.[26] Several recently discovered breaches involving data held by the Office of Personnel Management ("OPM") have put millions of individuals at risk of identity theft.[27] In June of 2015, the OPM, which maintains records for current, former, and prospective federal employees, notified approximately 4 million federal employees that the computer systems of a background investigative services contractor had been hacked.[28] The OPM initially estimated that the personally identifiable information of 4 million federal employees may have been stolen, giving the hackers access to biometric fingerprints; residency and educational history; employment history; family information and other personal information; health, criminal and financial history; and other details, such as foreign trips taken, names of neighbors and close friends, and more.[29] Recent reports indicate that the background investigative and personal data of two of OPM's contractors - KeyPoint and U.S. Investigations Services - were hacked, affecting approximately 25.7 million records belonging to 22.1 million current, former and prospective federal employees, as well as their spouses or partners.[30] To date, the expenses incurred by the federal government in connection with these breaches include temporary credit monitoring services, fraud protection, and identity theft insurance for roughly 28 million individuals. The true cost of the massive OPM date breach remains to be seen since multiple lawsuits have been filed by federal employees.[31] These lawsuits are discussed in further details in Part V, *infra*.

IV. REGULATORY FRAMEWORK

In the United States, unlike other countries, lawmakers have not enacted a uniform law that protects data. Instead, the collection, storage, release, or destruction of data is regulated on both the state and federal level, and such regulations are primarily enforced by industry, *e.g.*, business industry, health industry, financial services industry, or public utilities[32]; activity, *e.g.*, electronic communication, electronic marketing, surveillance, conducting background checks;

---

[25] *Id.*

[26] Privacy Rights, *Chronology of Data Breaches*, *supra* note 6.

[27] *Id.* (A search for breaches disclosed during the last two years indicates that breaches have been reported by the following federal agencies: the Federal Deposit Insurance Corporation, the Internal Revenue Service, the U.S. State Department, the U.S. Weather Service, the U.S. Postal Service, and the Department of Veterans Affairs).

[28] David Bisson, *The OPM Breach: Timeline of a Hack*, THE STATE OF SECURITY, July 10, 2015, at http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/.

[29] Press Release, U.S. Office of Personnel Management, OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats (July 9, 2015) (*available at* https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/).

[30] Jedidiah Bracy, *21.5 Million Breached In Second OPM Hack; Director Resigns*, PRIVACY TECH, ¶ 2 (July 10, 2015), https://iapp.org/news/a/21-5-million-breached-in-second-opm-hack/.

[31] Zach Noble, *Full dollar cost of OPM breach still a giant unknown*, FCW, ¶ 3, 5 (September 2015) (*available at* https://fcw.com/articles/2015/09/10/opm-breach-cost.aspx).

[32] Lisa J. Sotto & Aaron P. Simpson, *Data Protection & Privacy 2015, United States, in* GETTING THE DEAL THROUGH 208 (Rosemary P. Jay, cont. ed., 2014); *see also* Natasha Singer, *An American Quilt of Privacy Laws, Incomplete*, THE NEW YORK TIMES (March 30, 2013).

the type of data, *e.g.*, cancer, genetic, HIV/AIDS, sexual assault, mental health, immunizations, federal tax, customer records of a government-operated utility, or government benefit recipient information[33]; or the status of the individual, *e.g.*, a minor, an elected official, or a government employee.[34] This piecemeal approach is why the legislative framework for the protection of individually identifying information is often compared to a patchwork quilt.[35] Consequently, there are numerous state and federal laws that regulate data privacy with different requirements depending on the regulated industry, entity, activity or status of the individual.

Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation that requires private, governmental or educational entities to notify individuals when personally identifiable information has been breached.[36] Some states impose civil penalties or authorize a private right of action against a public entity that fails to safeguard the privacy, security or integrity of identifying information.[37] In addition, the definition of personally identifiable information varies depending on the applicable law or regulation. In the security breach notification law context, for example, personal identifiable information generally includes an individual's name in conjunction with the individual's Social Security number, driver's license number, or bank account number.[38]

---

[33] *See, generally,* TEX. HEALTH & SAFETY CODE § 82.009(a) (West Supp. 2016) (relating to confidentiality of cancer reports, records and information obtained the Texas Board of Health); Genetic Information Nondiscrimination Act of 2008 ("GINA") Pub. L. No. 110-233, TEX. INS. CODE § 546.102 (West 2009), TEX. LABOR CODE § 21.403 (West 2015) and TEX. OCC. CODE § 58.102 (West 2012) (relating to confidentiality of records containing genetic information); TEX. HEALTH & SAFETY CODE § 81.103(a) (West 2010 and Supp. 2016) (relating to confidentiality of HIV/AIDS test results); TEX. GOV'T CODE §§ 420.010 and 420.071 (West 2016) (relating to identification of, and communications with, sexual assault victims); TEX. HEALTH & SAFETY CODE § 611.002(a) (West 2010) (relating to communications between a patient and professional for diagnosis, evaluation or treatment of any mental or emotional condition or disorder, including alcoholism or drug addiction); TEX. HEALTH & SAFETY CODE § 161.0073 (West 2010 and Supp. 2016) (relating to confidentiality of immunization records); TEX. UTIL. CODE § 182.052 (West 1998 and Supp. 2016)) (relating to confidentiality of customer records held by a government-operated utility); 26 U.S.C. § 6103(a) (2016) (relating to confidentiality of federal tax return and tax return information); 7 C.F.R. § 272 (2016); 45 C.F.R. § 205.50 (2016); 42 C.F.R. §§ 431.300, 457.1110 (2016) (concerning recipients of government benefits, such as Medicaid, the Supplemental Nutrition Assistance Program, Temporary Assistance for Needy Families, or the Children's Health Insurance Program by the Health and Human Services Commission, its designee(s), third party(ies), or business associates).

[34] *See, e.g.*, TEX. ALC. BEV. CODE § 106.117(d) (West 2007), TEX. CODE OF CRIM. PROC. arts. 44.2811, 45.0217(a), 63.015(b), 63.017 (West 2006 and Supp. 2016); TEX. EDUC. CODE § 25.002(b) (West 2012); TEX. FAM. CODE §§ 33.002(f), 33.003(k), (*l*) and (*l*-2), 33.004(c), 54.033(f), 54.04(w)(3), 58.005, 58.007(b) and (c), 58.00711(b), 58.0072, 58.106, 58.307 and 85.007 (West 2014 and Supp. 2016); TEX. GOV'T CODE § 422.004 (West 2012); TEX. OCC. CODE § 159.005 (West 2012) (relating to confidentiality or release of information involving a minor, child or juvenile).

[35] *See, e.g.*, Sotto & Simpson, *supra* note 32, at 208.

[36] National Conference of State Legislatures, *Security Breach Notification Laws* (January 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [hereinafter NCSL, *Breach Notification Laws*].

[37] *See, e.g.*, The Identity Theft Enforcement and Protection Act, codified at TEX. BUS. & COMM. CODE §§ 521.001 – 521.152 (West 2012 and Supp. 2016) and The Texas Medical Records Privacy Act, codified at TEX. HEALTH & SAFETY CODE §§ 181.001 – 181.207 (West 2010 and Supp. 2016).

[38] NCSL, *Breach Notification Laws*, *supra* note 36.

A. Texas Laws

In Texas, a local government can face civil penalties if it does not comply with state breach notification laws. The key state laws that regulate the disclosure of identifiable information owned or maintained by a local government are (1) The Identity Theft Enforcement and Protection Act (the "ITEPA"); (2) The Texas Medical Records Privacy Act ("TMRPA"); and (3) other state laws that protect social security numbers, biometric identifiers, and crime victim information. The key terms under these laws are "sensitive personal information" and "protected health information." This section of the paper provides an overview of Texas laws that regulate the collection, storage, release, or destruction of data containing certain identifiable information held by a local government.[39]

1. The Identity Theft Enforcement and Protection Act

The ITEPA imposes a duty on businesses to protect and safeguard sensitive personal information and requires the notification of an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information. While the ITEPA does not expressly apply to local governments, Chapter 205 of the Local Government Code incorporates key provisions of the ITEPA. Thus, a local government must comply with the breach notification requirements of the ITEPA.[40]

a. Definition of Sensitive Personal Information

The ITEPA covers a business that collects or maintains "sensitive personal information" of Texas residents in its regular course of business.[41] The ITEPA broadly defines sensitive personal information to cover an individual's first name or first initial and last name in combination with any one or more of the following unencrypted pieces of information:

- Social Security number;
- Driver's license number or government-issued identification number; and
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.[42]

Sensitive personal information also covers information that identifies an individual and relates to (i) the physical or mental health or condition of the individual, (ii) the provision of health care to the individual, or (iii) the payment for the provision of health care to the individual.[43] However,

[39] This paper uses the term "identifiable information" to generally refer to all types of information that identifies an individual, whether financial, medical, criminal, or consumer records are involved. The regulation of a local government that collects and maintains information related to critical infrastructure is beyond the scope of this paper.
[40] TEX. LOC. GOV'T CODE § 205.010 (West 2008 and Supp. 2016).
[41] TEX. BUS. & COM. CODE § 521.052.
[42] *Id*.
[43] TEX. BUS. & COM. CODE § 521.002(a)(2) (West 2015).

sensitive personal information does not include "publicly available information that is lawfully made available to the public from the federal government or a state or local government."[44]

ITEPA requires a covered business to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business."[45] Additionally, covered businesses are required to destroy or arrange for the destruction of records that contain sensitive personal information by (1) shredding, (2) erasing, or (3) otherwise modifying the sensitive personal information contained in the records in a manner "to make the [personal] information unreadable or indecipherable through any means."[46] State law does not impose a similar duty on local governments. However, a duty to implement procedures to prevent the unlawful use or disclosure of sensitive personal information may be imposed on a local government if the local government uses, stores or exchanges medical information. A local government that uses, stores or exchanges medical information may be a "covered entity" under HIPAA or TMRPA.

b. Definition of Breach

ITEPA defines a "breach of system security" as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a business, including data that is encrypted if the person accessing the data has the key required to decrypt the data. However, good faith acquisition of sensitive personal information by an employee or agent of the person is not a breach unless the information is used or disclosed, whether by the employee, the agent, or any other individual, in an unauthorized manner.[47]

Certain local governments must comply with provisions of the ITEPA. Specifically, a local government that owns, licenses, or maintains computerized data that includes sensitive personal information must comply with the notification requirements of ITEPA to the same extent as a person who conducts business in Texas in the event of a breach of system security.[48] Similarly, a state agency that owns, licenses, or maintains computerized data that includes sensitive personal information must comply with the notification requirements of ITEPA in the event of a breach of system security.[49]

c. Breach Notification Requirements

A business, local government or state agency that owns, licenses, or maintains computerized data that includes sensitive personal information must disclose a breach after discovering or receiving notice of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

[44] *Id.* § 521.002(b).
[45] *Id.* § 521.052(a).
[46] *Id.* § 521.052(b).
[47] *Id.* § 521.052(a).
[48] TEX. LOC. GOV'T CODE § 205.010(b).
[49] TEX. GOV'T CODE § 2054.1125(b) (West 2016).

The required disclosure must be made "as quickly as possible" unless a law enforcement agency requests a delay in notification to avoid compromising an ongoing investigation or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.[50] If the individual whose sensitive personal information was breached is a resident of another state, the required notice may either be provided under that state's law or under Texas law.[51] If an affected individual resides in a state without a data breach notification statute, the individual must be notified in accordance with Texas law. Currently, the states that lack data breach notification requirements are Alabama, New Mexico, and South Dakota.[52]

A business, local government, or state agency may provide the required notice via either: (i) written notice mailed to the last known address of the individual; or (ii) electronic notice, only if the notice is provided in accordance with the federal Electronic Records and Signatures in Commerce Act.[53] If a business, local government or state agency is required by ITEPA to notify more than 10,000 individuals of a breach of system security at one time, the business, local government or state agency must also notify, without unreasonable delay, each consumer reporting agency that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.[54]

Alternatively, if the business, local government or state agency demonstrates that the cost of providing notice would exceed $250,000, there are more than 500,000 affected individuals, or the business, local government or state agency does not have sufficient contact information for the affected individuals, the notice may be given by:

- E-mail if maintained for the affected individuals;
- Conspicuous posting of the notice on the business, local government or state agency's website; or
- Notice published in or broadcast on major statewide media.[55]

A business, local government or state agency that maintains separate notification procedures as part of an information security policy for the treatment of sensitive personal information may provide the required notice in accordance with the notification methods of such a policy, but it must adhere to the timing requirements for notice under ITEPA.[56]

d. Enforcement

The Attorney General may bring a civil suit for damages or an injunction. A person who violates the statute is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. A person who fails to take reasonable action to comply with notification requirements is liable to the state for a civil penalty of not more than $100 for each

[50] TEX. BUS. & COM. CODE § 521.052(c) and (d).
[51] *Id.* § 521.052(b-1).
[52] NCSL, *Breach Notification Laws*, *supra* note 38.
[53] TEX. BUS. & COM. CODE § 521.052(e); *see also* 15 U.S.C. § 7001 (2016).
[54] TEX. BUS. & COM. CODE § 521.052(h).
[55] *Id.* § 521.052(f).
[56] *Id.* § 521.052(g).

individual to whom notification is due for each consecutive day the person fails to take reasonable action to notify with a maximum penalty of $250,000 for a single breach. These provisions, arguably, do not apply to a local government.[57]

If it appears to the Attorney General that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the Attorney General may bring an action against the person for a temporary restraining order or by a permanent or temporary injunction. These provisions, arguably, do apply to a local government.[58] A violation of ITEPA is also a deceptive trade practice under the Texas Deceptive Trade Practices Act; however, the Texas Deceptive Trade Practices Act does not apply to a local government.[59]

2. Texas Medical Records Privacy Act

The TMRPA, in some respects, provides more protection for individual privacy than its federal counterpart, Title 2 of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, the Privacy Rule, the Security Rule, the Enforcement Rule, and the Omnibus Rule (hereinafter referred to collectively as "HIPAA"). TMRPA incorporates by reference a few key terms of HIPAA and the Privacy Rule.[60] TMRPA provides additional protections by defining key terms more broadly, establishing additional protections for individuals, and imposing stiffer penalties for non-compliance.[61]

One key difference between HIPAA and TMRPA is that Texas law imposes a broader definition of a "covered entity," thereby regulating additional entities beyond HIPAA. A local government that merely uses, stores or exchanges medical information is likely a "covered entity" under TMRPA. In this paper, these types of local governments are referred to as a TMRPA covered entity. It is important to note that a local government that is subject to TMRPA, but that is not subject to HIPAA because it is not a health plan, health provider or health information exchange, only needs to comply with TMRPA and does not need to also comply with HIPAA, HITECH and related administrative regulations.[62]

Another key difference is that state law does not impose any breach notification requirements on a TMRPA covered entity. That is, in the event of a breach of protected health information, a TMRPA covered entity does not need to notify an affected individual unless the breach involves computerized records that indicate the physical or mental health or condition of an individual, the provision of health care to the individual, or the payment of health care services because the breach of this type of medical information is regulated by ITEPA. A local

[57] *Id.* § 521.151(a) and (a-1).
[58] *Id.* § 521.151(b).
[59] *Id.* § 521.052(g).
[60] The regulations referred to as The Privacy Standards are located at 45 C.F.R. Part 160, 162, and 164, Subparts A and E, as amended by HITECH.
[61] Cheryl Camin Murray, *Don't Mess with Texas – A Summary of State Laws Concerning Health Information*, HEALTHCARE DAILY (May 1, 2013).
[62] *New Developments in Safeguarding Protected Health Information During 2014* Submitted to the House Public Health Committee and the Senate Health and Human Services Committee by the Health and Human Services Commission (December 2014).

government that is a covered entity under HIPAA because it is a health plan, health provider, or health information exchange, should consult Part IV.B.1. of this paper, which summarizes federal regulations regarding data security for a local government that is regulated as a covered entity under HIPAA.[63] In this paper, these types of local governments are referred to as a HIPAA covered entity.

a. Definition of Covered Entity

As indicated, TMRPA defines "covered entity" broadly enough to include many entities that are not regulated under HIPAA. TMRPA defines a covered entity as any person who for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis:

- Assembles, collects, analyzes, uses, evaluates, stores, or transmits protected health information;
- Comes into possession of protected health information; or
- Obtains or stores protected health information under TMRPA.[64]

By definition, a covered entity expressly includes a health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, or health care provider, or person that maintains an Internet site.[65] A TMRPA covered entity also includes an employee, agent, or contractor of a covered entity if the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.[66]

b. Definition of Protected Health Information and Individually Identifiable Health Information

TMRPA incorporates definitions from HIPAA and the Privacy Standards for terms that are referenced in TMRPA but that are not expressly defined.[67] Protected health information is one such term. Thus, for purposes of TMRPA, "protected health information" means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any form or medium by a covered entity or its business associate.[68] Protected health information does not include "individually identifiable health information": (i) in education records covered by the Family Educational Rights and Privacy Act ("FERPA") that are available to parents or education records for those over age 18 or in college; or (ii) in employment records held by a covered entity in its role as employer unless the employer's activities involve the re-identification, marketing, the sale, or the electronic disclosure of protected health information.[69] For a governmental unit that is a TMRPA

[63] 45 C.F.R. § 160.103 (2016).
[64] TEX. HEALTH & SAFETY CODE §181.001(b)(2)(A)-(C) (West 2010 and Supp. 2016).
[65] *Id.* § 181.001(b)(2)(A).
[66] *Id.* § 181.001(b)(2)(D).
[67] *Id.* § 181.001(a).
[68] 45 C.F.R. § 160.103.
[69] TEX. HEALTH & SAFETY CODE §§ 181.051, 181.151-181.154 (West 2010 and Supp. 2016).

covered entity, an individual's protected health information also includes information that reflects that an individual received health care from a governmental unit unless that information is subject to disclosure pursuant to Chapter 552 of the Government Code.[70]

Individually identifiable health information is another term that is referenced, but not defined, in TMRPA. Thus, a local government must look to HIPAA and the Privacy Standards for the definition of this term. Under the Privacy Standards, individually identifiable health information is a type of information collected from an individual, including demographic information that either identifies an individual or can be used to identify the individual and relates to:

- The past, present, or future physical or mental health or condition of an individual;
- The provision of health care to an individual; or
- The past, present, or future payment for the provision of health care to an individual.[71]

c. Definition of Breach

Recall that TMRPA incorporates definitions from HIPAA and the Privacy Standards for terms that are referenced in TMRPA but that are not expressly defined. TMRPA does not reference the term "breach," therefore, TMRPA does not incorporate the definition of breach from HIPAA or the Privacy Standards. Even though TMRPA does not impose any breach notification requirements, a local government that is a TMRPA covered entity is subject to data breach notification requirements. A comparison of the definition of individually identifiable health information and sensitive personal information shows that the definition of individually identifiable information is subsumed by the definition of sensitive personal information to the extent the information is maintained as computerized data. Under the ITEPA, "breach of system security" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a local government, including data that is encrypted if the person who acquires the data has the key to decrypt the data. A local government that owns, licenses, or maintains computerized data that identifies an individual and relates to: (1) the physical or mental health or condition of the individual; (2) the provision of health care to the individual; or (3) the payment for the provision of health care to the individual since such activities are regulated by, and thus fall under the umbrella of, the ITEPA.[72] To be clear, a local government that experiences a breach of computerized data that involves either sensitive personal information or individually identifiable information that it owns, licenses, or maintains, must comply with the breach notification requirements of ITEPA.

[70] *Id*. §181.006.
[71] 45 C.F.R. § 160.103.
[72] *See supra* Part IV.A.1.

d. Breach Notification Requirements

A local government that is a TMRPA covered entity must comply with the breach notification requirements under ITEPA if it is a TMRPA covered entity and experiences a breach of system security that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, or the payment for the provision of health care to the individual such that it compromises the security, confidentiality, or integrity of the information.[73]

e. Additional Requirements

Aside from complying with breach notification requirements, a TMRPA covered entity must comply with regulations that: (i) restrict the disclosure of protected health information in electronic format; (ii) restrict the use of protected health information for marketing purposes; (iii) prohibit the sale of protected health information; and (iv) mandate certain employee training. A TMRPA covered entity may not electronically disclose an individual's or employee's protected health information unless it provides both notice and authorization from the individual or the individual's legally authorized representative for *each* disclosure. A TMRPA covered entity may provide general notice by:

- Posting a written notice in the covered entity's place of business;
- Posting a notice on the covered entity's Internet website; or
- Posting a notice in any other place where individuals whose protected health information is subject to electronic disclosure are likely to see the notice.

A sample general notice is included in the Appendix. Authorization is not required if the disclosure is authorized or required by state or federal law. If the disclosure is not authorized or required by law, a separate authorization is required for every disclosure of protected health information in electronic format.

In addition, a TMRPA covered entity may not use or disclose protected health information for marketing purposes without first obtaining consent or authorization from the individual.[74] Written communications must explain the recipient's right to removal from the mailing list, and removal must be accomplished by TMRPA covered entity within 45 days after the receipt of the request.[75] TMRPA also imposes a blanket prohibition on selling protected health information. That is, a TMRPA covered entity may not disclose an individual's protected health information to anyone in exchange for direct or indirect remuneration.[76]

Finally, a TMRPA covered entity must train its employees on state and federal laws regarding the entity's use, storage or exchange of protected health information within 90 days after the employee is hired and within one year of a material change in law concerning protected

[73] TEX. LOC. GOV'T CODE § 205.010; TEX. BUS. & COM. CODE §§ 521.002(2), 521.053.
[74] TEX. HEALTH & SAFETY CODE § 181.152.
[75] *Id.* §§ 181.152(b)(2) and (c).
[76] *Id.* § 181.153.

health information. Each employee must sign a statement verifying the employee's training. TMRPA covered entity must maintain these signed statements for six years.[77]

f. Exceptions

TMRPA exempts many types of records from its regulations. What follows are the exceptions that are most likely to apply to a local government entity – exceptions that apply to records held as an employer, workers compensation records, certain medical records regarding juveniles, and certain records regarding crime victims. For information held by a local government in its scope as an employer, TMRPA imposes additional regulations on a TMRPA covered entity. Unlike HIPAA, TMRPA only provides for a partial exception for employer records. If an employer re-identifies the protected health information of its employees, markets the protected health information of its employees, sells protected health information of its employees, or electronically discloses the protected health information of its employees, it must comply with TMRPA when doing so.[78] However, with respect to workers compensation records, TMRPA does not apply to workers' compensation insurance, a function authorized by Title 5 of the Labor Code, or any person in connection with providing, administering, supporting, or coordinating any of the benefits under a workers' compensation self-insured program.[79] TMRPA also exempts an employee benefit plan and a covered entity or person acting in connection with an employee benefit plan.[80] The important takeaway for city attorneys is that a local government that re-identifies the protected health information of its employees, markets the protected health information of its employees or electronically discloses the protected health information of its employees must do so in accordance with TMRPA. *A local government cannot receive direct or indirect compensation in exchange for the protected health information of its employees.*

With respect to juveniles, TMRPA does not apply to "education records" covered by FERPA or other records accessible by an educational agency, such as law enforcement records created by a law enforcement unit of the educational agency or institution for law enforcement purposes.[81] In addition, TMRPA does not apply to an agency listed or described in Health and Safety Code, Section 614.017 that discloses, receives, transfers, or exchanges protected health information related to a special needs offender or a juvenile with a mental impairment in the custody of the agency for purposes of continuity of care and services.[82] Among the many entities listed in Section 614.017, local jails regulated by the Commission on Jail Standards, a municipal or county health department, and a hospital district and a judge with jurisdiction over juvenile or criminal cases are included.[83]

Finally, TMRPA does not apply to certain medical or law enforcement records held by a local government. Specifically, a local government does not have to comply with TMRPA when it creates, maintains or transmits protected health information in connection with providing,

[77] *Id.* § 181.101.
[78] *Id.* §§ 181.051 and 181.151-181.154.
[79] *Id.* § 181.154.
[80] *Id.* § 181.055.
[81] *Id.* § 181.058; 20 U.S.C. § 1232g(a)(4)(B) (2016) (excluding certain records held or accessible by an education agency from the definition of education records).
[82] TEX. HEALTH & SAFETY CODE § 181.055.
[83] *Id.* § 181.057; TEX. HEALTH & SAFETY CODE § 614.017 (West 2010 and Supp. 2016).

administering, supporting, or coordinating benefits regarding compensation to crime victims as provided by Code of Criminal Procedure, Chapter 56, Subchapter B.[84]

g. Enforcement

TMRPA authorizes the Texas Attorney General to institute an action for civil penalties due to TMRPA violations. The civil penalty imposed under TMRPA is capped at:

- $5,000 per violation per year committed negligently;
- $25,000 per violation per year if committed knowingly or intentionally; or
- $250,000 per violation if the covered entity knowingly or intentionally used the protected health information for financial gain.[85]

The total amount of a penalty assessed against a TMRPA covered entity due to a violation that involves the electronic disclosure of protected health information may be reduced and capped at $250,000 annually if the court finds that the disclosure was made to another covered entity for treatment, payment, health care operations, performing an insurance or health maintenance organization function or as otherwise authorized or required by state or federal law only if the court finds that: (i) the disclosed protected health information was encrypted or transmitted using encryption technology designed to protect against improper disclosure; (ii) the recipient of the protected health information did not use or release the protected health information; or (iii) at the time of the disclosure, the covered entity had developed, implemented, and maintained security policies, including the education and training of employees responsible for the security of protected health information.[86]

In a proceeding to impose an administrative or civil penalty due to the disclosure of individually identifiable health information, a covered entity may introduce, as mitigating evidence, evidence of the entity's good faith efforts to comply with: (i) state law related to the privacy of individually identifiable health information; or (ii) HIPAA and the Privacy Standards.[87] In determining a penalty imposed on a TMRPA covered entity that is licensed by a state agency, a court or state agency must consider the following factors:

- The seriousness of the violation, including the nature, circumstances, extent, and gravity of the disclosure;
- The covered entity's compliance history;
- Whether the violation poses a significant risk of financial, reputational, or other harm to an individual whose protected health information is involved in the violation;
- Whether the covered entity was certified at the time of the violation under Health & Safety Code, Section 182.108;

[84] *Id*. § 181.059.
[85] *Id*. § 181.201(b).
[86] *Id*. § 181.201(b-1).
[87] *Id*. § 181.205(a).

- The amount necessary to deter a future violation; and
- The covered entity's efforts to correct the violation.[88]

Unlike the ITEPA, TMRPA does not exempt a local government entity from civil penalties or other enforcement actions. Thus, a local government that uses, stores or exchanges medical information in its scope as an employer must comply with portions of TMRPA and a local government that is a TMRPA covered entity is exposed to significant liability if it violates TMRPA.

3. Motor Vehicle Records Disclosure Act

The MVRDA was to implement the provisions of the federal Driver's Privacy Protection Act ("DPPA"). These laws protect personal information contained in the motor vehicle records. The release and use of all personal information contained in a motor vehicle record is restricted and should be released only as authorized by state or federal law.

a. Definition of Personal Information

The Motor Vehicle Records Disclosure Act ("MVRDA") prohibits the disclosure and use of personal information contained in motor vehicle records unless authorized by the individual or by state or federal law.[89] The law applies to a political subdivision that compiles or maintains motor vehicle records, including the authorized agent or contractor of a political subdivision.[90] The MVRDA defines "personal information" as information that identifies a person, including:

- an individual's photograph or computerized image,
- social security number,
- driver identification number,
- name,
- address, but not the zip code,
- telephone number, and
- medical or disability information.

The term does not include (i) information about vehicle accidents, driving or equipment-related violations, or driver's license or registration status; or (ii) information contained in an accident report prepared under Transportation Code, Chapter 550 or 601.[91]

b. Required or Permitted Disclosure of Personal Information

Personal information obtained by a political subdivision must be disclosed for use in connection with: (i) motor vehicle or motor vehicle operator safety; (ii) motor vehicle theft; (iii) motor vehicle product alterations, recalls, or advisories; (iv) performance monitoring of motor vehicles, motor vehicle parts, or motor vehicle dealers; (v) motor vehicle market research

[88] *Id*. § 181.205(b).
[89] TEX. TRANS. CODE § 730.002 (West 2011).
[90] *Id*. § 730.003(1).
[91] *Id*. § 730.003(6).

activities, including survey research; or (vi) removal of non-owner records from the original owner records of motor vehicle manufacturers; (vii) child support enforcement; (viii) enforcement actions by the Texas Workforce Commission; and (ix) voter registration or the administration of elections.[92] In addition, a political subdivision must release personal information to a requestor if he or she has written consent from the person who is the subject of the information.[93] A political subdivision may release the (i) name and address; (ii) date of birth; and (ii) driver's license number for a permitted use as specified under Transportation Code, Section 730.007.

c. Resale or Redisclosure of Personal Information

Personal information released by a state agency or political subdivision may not be resold or re-disclosed unless it is to be used only as permitted by MVRDA. In addition, a recipient of personal information may not resell or redisclose the personal information in an identical or substantially identical format that the state agency or political subdivision disclosed such information to the recipient. A political subdivision, its agent or contractor must require a recipient of personal information to maintain a record of disclosures of resold or redisclosed information to an individual or entity. The record must include the permitted use for which personal information was resold or redisclosed. The record of disclosures and permitted uses must be maintained by the recipient for at least 5 years. Also, the person or entity must provide a copy of the record of disclosures and permitted uses to the political subdivision upon request.[94] A person who is convicted of a violation of MVRDA or an administrative regulation adopted by a state agency relating to the terms or conditions for release of personal information is ineligible to receive personal information under Transportation Code, Section 730.007.[95]

d. Enforcement

A violation of a requirement of MVRDA can result in civil and criminal penalties. Violations include falsifying statements, or knowingly, obtaining, disclosing, or using the information obtained from a motor vehicle record in violation of MVRDA. A civil or criminal penalty can be imposed on an individual, organization, or entity, who obtains, has access to, uses, releases, or rediscloses motor vehicle information in violation of MVRDA.[96] The state, a state agency, political subdivision, or an authorized agent or contractor of a state agency or political subdivision that compiles or maintains motor vehicle records is exempt from the enforcement provisions.[97]

e. Administrative Regulations

In addition to state law requirements that regulate a political subdivision's disclosure of motor vehicle records, state agencies that sell or provide access to driver records have

[92] *Id*. § 730.005 (West 2011 and Supp. 2016).
[93] *Id*. § 730.006.
[94] *Id*. § 730.013.
[95] *Id*. § 730.016.
[96] *Id*. §§ 730.013 and 730.015.
[97] *Id*. § 730.003(5).

promulgated administrative regulations that require a written service agreement with a local government when releasing motor vehicle record information.[98] A political subdivision should review agreements entered into with the Texas Department of Public Safety ("DPS") and the Texas Department of Motor Vehicles ("DMV") to determine whether it must comply with any breach notification or privacy requirements in addition to those imposed on political subdivisions via state and federal law. For instance, a standard agreement drafted by DPS requires a political subdivision to notify the agency within two calendar days of any inadvertent or unauthorized release, disclosure, breach, or compromise of driver records. An agency may hold a political subdivision responsible for ensuring that any party to which the political subdivision releases driver record information complies with all federal and state laws that regulate the release of such records. If a state agency determines that an improper disclosure of personal information has been made by any party that directly or indirectly obtained the driver record information from a political subdivision, the agency may terminate the agreement with the political subdivision.[99] If an agreement is terminated due to a violation of a clause or term of the agreement, it cannot enter into a subsequent agreement to obtain driver record information with either agency.[100] A copy of a standard Agreement for Governmental Entities with DPS is included in the Appendix. A copy of a standard Service Contract for Accessing Texas Motor Vehicle Records with DMV is also included in the Appendix.

4. Other State Laws

Texas laws also restrict the use or disclosure of other types of information. Provisions of the Business and Commerce Code regulate the disclosure of (i) social security numbers to municipally owned utilities; (ii) identifying financial information; (iii) biometric identifiers; and (iv) crime or accident victim information.

a. Social Security Numbers held by Municipally Owned Utility

A municipally owned utility may not require an individual to disclose the individual's social security number to obtain utility services unless the municipally owned utility adopts a privacy policy that includes:

- How personal information is collected;
- How and when the personal information is used;
- How the personal information is protected;
- Who has access to the personal information; and
- The method of disposal of the personal information.[101]

The municipally owned utility must make the privacy policy available to the individual and maintain the confidentiality and security of all disclosed social security numbers pursuant to the privacy policy.[102]

---

[98] 37 Tex. Admin. Code §§ 15.141-15.148 (2016); 43 Tex. Admin. Code §§ 217.121-217.124 (2016).
[99] *See* 37 Tex. Admin. Code § 15.143.
[100] *See id.* § 15.146.
[101] TEX. BUS. & COM. CODE §§ 501.051(3), 501.052(a)(1) and (b) (West 2015) .
[102] *Id.* § 501.052(a)(2) and (3).

A municipally owned utility that violates this requirement is liable for a civil penalty in an amount not to exceed $500 for each calendar month during which a violation occurs. The attorney general or the district attorney in the county in which the violation occurs may bring an action to recover an imposed civil penalty. Either the Attorney General or the district attorney of the county in which the violation occurs may bring an action to recover the civil penalty. In addition, the attorney general may bring an action in the name of the state to restrain or enjoin a person from violating the restriction.[103]

b. Identifying Financial Information

A person, including a local government, who accepts a credit card or debit card to transact business may not print on a receipt provided to a cardholder more than the last four digits of the credit card or debit card account number or the month and year that the credit card or debit card expires. A civil penalty in an amount not to exceed $500 for each calendar month during which a violation occurs. Either the Attorney General or the district attorney of the county in which the violation occurs may bring an action to recover the civil penalty. In addition, the attorney general may bring an action in the name of the state to restrain or enjoin a person from violating the restriction.[104]

c. Biometric Identifiers

A person, including a local government, may not capture a biometric identifier, defined as a retina, iris scan, fingerprint, voiceprint, or record of hand or face geometry, of an individual for a commercial purpose unless the person informs the individual before capturing the biometric identifier and receives the individual's consent to capture the biometric identifier. A person who possesses a biometric identifier of an individual that is captured for a commercial purpose may not sell, lease, or otherwise disclose the biometric identifier to another person unless: (i) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death; (ii) the disclosure completes a financial transaction that the individual requested or authorized; (iii) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552 of the Government Code; or (iv) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant.[105] Commercial purpose is typically defined as a purpose that is intended to result in a profit or other tangible benefit.

In addition, a person who possesses an individual's biometric identifier is captured for a commercial purpose, the person must use reasonable care when storing or transmitting the biometric identifier and protect it from disclosure in a manner that, at a minimum, is as protective as the manner that the person stores, transmits, and protects any other confidential information it possesses. A person who possesses a biometric identifier of an individual that is captured for a commercial purpose must destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier

[103] *Id.* § 501.053.
[104] TEX. BUS. & COM. CODE §§ 1.201(27) (West 2009 and Supp. 2016) and 502.002 (West 2015).
[105] TEX. BUS. & COM. CODE §§ 1.201(27) and 503.001 (West 2015).

expires unless the biometric identifier is used in connection with an instrument or document that is required by another law to be maintained for a period longer than one year, in which case the person who possesses the biometric identifier must destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law. When a biometric identifier has been collected for security purposes by an employer, the purpose for collecting the identifier is presumed to expire upon termination of the employment relationship. A person who does not comply with these provisions is subject to a civil penalty of $25,000 per violation in an enforcement action initiated by the attorney general.[106]

d. Crime Victim Information

A person, including a local government, who possesses crime victim or motor vehicle accident information that is obtained from a law enforcement agency may not use the information to contact, for the purpose of soliciting business, any of the following individuals: (i) a crime victim or a family member of the victim; (ii) a person, or a family member of the person, who was involved in a motor vehicle accident. A person, including a local government, who possesses crime victim or motor vehicle accident information that is obtained from a law enforcement agency may not sell information to another person for financial gain.[107]

5. Criminal Enforcement

A review of Texas laws that impose criminal liability for the unauthorized use, inspection or disclosure of information that is confidential by law has recently been addressed in a seminar paper and presentation to the Texas City Attorneys Association.[108] Of particular significance to attorneys who advise local governments is that there are in excess of 700 statutes that limit the disclosure of information or that make certain information confidential.[109] City attorneys and outside counsel who advise cities should review the statutes listed in this paper to ensure that city officers and employees are not inadvertently exposing themselves to criminal liability or civil penalties.

B. FEDERAL LAWS AND INDUSTRY STANDARDS

On the federal level, lawmakers have not implemented an omnibus data protection law. Instead, there are specific privacy laws for the types of citizen and consumer data that are deemed to the most sensitive, such as financial, insurance and medical information; information about children and students; telephone, internet and other electronic communications; credit, consumer, and background investigation reports. Most of these federal laws apply to federal agencies and businesses, however. There are only a few federal laws that impose data protection requirements on a local government. This Section summarizes a few of the federal laws that regulate how a local government collects, discloses and maintains individually identifying

[106] *Id*. § 503.001(d).
[107] TEX. BUS. & COM. CODE §§ 1.201(27) and 504.002 (West 2015).
[108] Miles K. Risley, *The Most Dangerous Thing we do every Day is hitting "Send": Criminalized Information Transfer*, TEXAS CITY ATTORNEYS ASSOCIATION CONFERENCE (2015).
[109] *Id*. at 5.

information. This Section also reviews industry standards that regulate the collection of information in connection with credit card transactions.

1. Health Information Portability and Accountability Act

HIPAA establishes national standards regarding health information privacy. It applies to covered health entities and to business associates. HIPAA regulates the use, storage and disclosure of protected health information, which encompasses individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. HIPAA establishes minimum protection for an individual's health information. HIPAA does not preempt a state law that imposes stricter requirements to safeguard the confidentiality, integrity and availability of protected health information.

As discussed, a local government that merely uses, stores, or exchanges medical information is likely a "covered entity" under TMRPA. A local government may also be regulated by HIPAA as a covered entity. A local government is subject to the requirements of HIPAA and must maintain the confidentiality of protected health information that it creates, transmits, uses, or maintains if it meets the definition of a covered entity as either a health plan or a health care provider.[110] A local government meets the definition of a "health plan" if it is self-insured with greater than fifty participants or if it sponsors a group health plan with greater than fifty participants and receives more than just enrollment/disenrollment and summary health information.[111] A local government meets the definition of a "health care provider" if it operates a fire department with first responders who provide emergency or ambulatory services.[112]

To comply with HIPAA, a local government must:

- Maintain the confidentiality of protected health information;
- Designate a Privacy Officer to receive complaints, coordinate compliance with respect to an individual's right to access his or her protected health information and ability to amend his or her protected health information, and issue a Notice of Privacy Practices;
- Designate a Security Officer to be responsible for ensuring that administrative, technical and physical safeguards are in place to safeguard the confidentiality, integrity, and availability of protected health information;
- Implement policies and procedures that comply with the Privacy Standards of HITECH;
- Conduct a risk assessment; and
- Implement policies and procedures that comply with the Security Standards of HITECH.[113]

[110] 45 C.F.R. § 164.502(a) (2016).
[111] 45 C.F.R. § 160.103.
[112] *Id*.
[113] 45 C.F.R. Part 164, Subpart C and Subpart E (2016).

The Privacy Rule requires a local government that is a HIPAA covered entity to permit individuals to access their medical records and submit a request to correct any errors in their records. The disclosure of medical information is allowed without an individual's permission for treatment, billing, and other related operations. However, all other disclosures require the written permission of the individual. A local government that is a HIPAA covered entity must also track all disclosures of protected health information and inform an individual of any use of that information. A local government that is a HIPAA covered entity must make reasonable efforts to keep communications regarding protected health information confidential.[114]

A local government that is a HIPAA covered entity performs both covered and non-covered functions. Therefore, it can minimize the scope of its coverage under HIPAA by declaring itself a "hybrid entity."[115] For a local government to establish itself as a hybrid entity, a local government should adopt a resolution that identifies those departments that create, transmit, use, or maintain protected health information and designate such departments as a health care component. Once the resolution has been adopted, only the designated departments of the local government are required to comply with HIPAA.[116]

OCR and the Texas Attorney General are authorized to enforce HIPAA. In addition to instituting an action for injunctive relief to restrain a violation under HIPAA or TMRPA, OCR and the Texas Attorney General are authorized to impose civil monetary penalties against a local government that is a HIPAA covered entity. The allowable civil penalties imposed under HIPAA are set forth below in Table 1, below.[117]

Table 1: Civil Penalties for HIPAA Violations by Covered Entity or Business Associate

Culpability for Violation	Minimum per HIPAA Violation	Maximum for Identical Violation of same Provision per calendar year
Did not know and, by exercising reasonable diligence, would not have known a violation occurred	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation occurred due to a reasonable cause and not willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation occurred due to willful neglect – corrected in timely manner	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million

[114] 45 C.F.R. § 164.522(b).
[115] 45 C.F.R. §§ 160.103, 164.105.
[116] 45 C.F.R. § 164.105(a)(1) and (a)(2)(iii)(D) (2016).
[117] 45 C.F.R. § 160.404.

Violation occurred due to willful neglect – not timely corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

While HIPAA protects the health information of individuals, it does not create a private cause of action for an individual affected by a HIPAA violation.

2. Privacy Act of 1974

The Privacy Act of 1974 regulates the federal government's collection and disclosure of personal information. For the most part, a local government entity is not subject to the Privacy Act of 1974. A local government must, however, comply with the social security number usage restrictions.[118] The social security number usage restrictions prohibit a federal, state, or local government agency from requiring an individual to provide his or her social security number to receive a right, benefit, or privilege provided by law. The restriction on collecting an individual's social security number does not apply to a required disclosure pursuant to federal law or to a system of records that existed before January 1, 1975. For instance, federal law permits a social security number to a governmental entity pursuant to a written request in connection with a civil or criminal law enforcement activity authorized by law.[119] When a government agency requests disclosure of a social security number, it must notify the individual whether the disclosure is mandatory or voluntary, what law authorizes the government agency to request the social security number, and how the social security number will be used.[120]

3. Driver's Privacy Protection Act

The DPPA restricts the release and use of personal information contained in motor vehicle records. The DPPA is codified at Chapter 123 of Title 18 of the United States Code.[121] As addressed in Part IV, A. 3., *supra*, the MVRPA adopts the provisions of the DPPA.

4. Federal Tax Information

The Internal Revenue Service ("IRS") requires a state or local government that legally receives federal tax information from either the IRS, a secondary source, or through an IRS-approved exchange agreement to protect federal tax information according to strict security guidelines.[122] Therefore, an employee of a federal, state or local agency who works with federal tax returns and tax return information must protect this information from unauthorized disclosure. An unauthorized disclosure occurs when an entity or individual with authorization to receive federal tax information discloses it to another entity or individual who does not have authority and a "need-to-know." A local government that is authorized to receive federal tax

[118] 5 U.S.C. § 552a (2016).
[119] *Id*. § 552a(b)(7) .
[120] *Id*. § 552a note "Disclosure of Social Security Number."
[121] 18 U.S.C. §§ 2721 – 2725 (2016).
[122] 26 USC §§ 6103(d), (*l*)(6), (7) and (8) (2016); *see also* INTERNAL REVENUE SERVICE, PUBLICATION 1075, TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES (2014).

information must also establish a record of requests for the disclosure of federal tax information that it receives.[123]

5. Data Security Standard

The Data Security Standard ("DSS") is a set of comprehensive requirements to enhance payment account data security that is administered by a consortium of the major credit card companies referred to as the Payment Card Industry Security Standards Council ("PCI"). The industry standards are imposed on entities via user agreements. The DSS applies to an entity that stores, processes or transmits cardholder data. Compliance is required for *any entity* that accepts payment cards at point of service – even if it processes only one payment transaction. The extent to which a local government must comply with the DSS depends on the amount of credit card transactions that it processes. A local government that suffers a breach and is not in compliance with the DSS is subject to paying penalty fees.[124]

The DSS requires a local government that stores, processes or transmits cardholder data to build and maintain a secure network and system by installing and maintaining a firewall configuration to protect cardholder data and prohibits the use of vendor-supplied defaults for system passwords and other security parameters; protect cardholder data by protecting stored cardholder data; encrypt transmission of cardholder data across open, public networks; maintain a vulnerability management program by protecting all systems against malware and regularly update antivirus software or programs and developing and maintaining secure systems and applications; implement strong access control measures by restricting access to cardholder data by business need to know and identifying and authenticating access to system components, and restricting physical access to cardholder data; regularly monitor and test networks by tracking and monitoring all access to network resources and cardholder data; regularly test security systems and processes by maintaining an information security policy by maintaining a policy that addresses information security for all personnel.[125]

V. LITIGATION

Data privacy litigation is an evolving area of law. To establish standing, a plaintiff must "prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision." With respect to data privacy litigation, the courts have typically held that a fear of future harm, alone, is insufficient to establish standing. Even where sufficient personally identifiable information has been disclosed to permit an unauthorized user to make fraudulent charges, courts generally require a plaintiff to plead actual unauthorized charges, identity theft, or fraud in order to establish an initial showing of harm.[126] Thus, the "injury-in-fact" requirement of Article III

[123] 26 USC § 6103(p)(4)(A).
[124] Payment Card Industry, *PCI Data Security Standard Requirements and Security Assessment Procedures, v3.2*, 5 (2016).
[125] *Id.*
[126] *See, e.g., Peters v. St. Joseph Servs. Corp.*, 474 F. Supp. 3d 847, 854 (S.D. Tex. 2015) (finding alleged future harm "speculative" where disclosed information included social security numbers, addresses, medical records and bank account information, and where illicit credit card purchase was declined).

standing has been a significant barrier to plaintiffs in data breach litigation. The Supreme Court's decision in *Clapper v. Amnesty International* provides the basic test regarding whether a plaintiff meets the injury-in-fact requirement to establish Article III standing - that "threatened injury must be certainly impending to constitute injury in fact" or if there is a "substantial risk" that the harm is going to occur.[127] A handful of data-breach cases, however, have survived threshold standing challenges in the Seventh and Ninth Circuits. In these cases, the plaintiffs were able to allege injury beyond a fear of future harm.[128]

In addition to alleging harm beyond a general fear of future harm, a number of federal statutes applicable to state and local government, including the DPPA, authorize an individual to sue based on a statutory violation. The Fair Credit Reporting Act ("FCRA"), which requires a consumer reporting agency to "follow reasonable procedures to assure maximum possible accuracy" of information used for employment purposes, is one such statute. Thomas Robins sued Spokeo, a "people search engine" that relies on data aggregation, alleging violations of the FCRA due to the company publishing inaccurate personal information about him on its website. The Ninth Circuit reversed the district court's dismissal for lack of standing, concluding that Robins' alleged injury was sufficient to confer standing because violations of the plaintiff's statutory rights adequately alleged a concrete and particularized injury.[129]

In April 2015, the U.S. Supreme Court granted certiorari on the issue of whether Congress may confer Article III standing upon a plaintiff by authorizing a private right of action based on a violation of a federal law.[130] In a 6-2 opinion, the Supreme Court concluded that the Ninth Circuit failed to determine whether Robins suffered a concrete harm. The Supreme Court acknowledged that while injuries may be intangible, just because Congress grants a private cause of action does not mean an individual has established injury-in-fact. In remanding the case, the Court did not rule out the possibility that the risk of real harm can solely satisfy the concreteness requirement. Thus, a data privacy litigant must still establish a concrete harm apart from a bare procedural violation of a statute.[131]

Another data privacy case to watch are the lawsuits arising out of the massive OPM data breach. At least two class action lawsuits and over a dozen other lawsuits have been filed against the OPM over the massive breach.[132] The cases have been consolidated and transferred to the U.S. District Court for the District of Columbia. The American Federation of Government

---

[127] *Clapper v. Amnesty International*, 133 S. Ct. 1138, 1147 (2013) (citing *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)).

[128] *In re Adobe Systems, Inc. Privacy Litig*., 2014 WL 4379916 (N.D. Cal. 2014) (finding that plaintiffs sufficiently alleged concrete injury where hackers specifically targeted personally identifiable information after an intrusion, used Adobe's own decryption keys and posted personally identifiable information on the Internet); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig*. (Sony II), 996 F. Supp. 2d 942, 962 (S.D. Cal. Jan 21, 2014) (concluding that plaintiffs successfully alleged injury-in-fact where their personal information was collected by Sony and was subsequently wrongfully disclosed due to an unauthorized intrusion); *Corona v. Sony Pictures Entm't Inc*., 2015 WL 3916744 (C.D. Cal. 2015) (alleged theft and publication of personally identifiable information on online file-sharing website is sufficient to establish Article III standing).

[129] *Robins v. Spokeo, Inc*., 742 F.3d 409 (9th Cir. 2014).

[130] *Spokeo, Inc. v. Robins*, 135 S. Ct. 1892 (2015).

[131] *Id*.

[132] Plaintiff's Consolidated Amended Complaint *In Re: U.S. Office of Personnel Management Data Security Breach Litigation* U.S. Dist. Court, District of Columbia (March 14, 2016).

Employees and the National Treasury Employees Union allege that the OPM and its contractors violated the 1974 Privacy Act, the Federal Information Security Management Act, the Federal Information Security Modernization Act, the Administrative Procedure Act, the Fair Credit Reporting Act, and that OPM's and its contractor's actions and inactions constituted negligence, negligent misrepresentation and concealment, invasion of privacy, and breach of contract by neglecting to secure employees' personal data, which resulted in financial and emotional harm. The litigants seek, in part, that the federal government provide the affected individuals with lifetime credit monitoring services, fraud protection, and identity theft insurance.[133] A key issue in the OPM litigation is likely to be whether the risk of real harm can satisfy the concreteness requirement for Article III standing.

VI. CONCLUSION

A city is obligated to ensure the privacy, security and integrity of data it collects. Public entities hold massive amounts of personal and business data, making them a target for criminals seeking financial gain, cyber espionage, or hacktivism. Yet, the cybersecurity efforts of public entities rank below that of other major industries. Regardless of whether the goal of the cyber criminal is monetary or to gather intel, a breach can inflict a great deal of harm on individuals, businesses, and the public sector. Due to the numerous state and federal laws that regulate data privacy, a public entity must comply with industry regulations, laws that regulate financial and medical activities, laws that regulate the type of data collected, and laws that restrict the disclosure of information based on the status of the individual. In addition, a public entity must comply with various regulations imposed on the state and federal levels, as well as by state agencies and industries via user agreements. The "injury-in-fact" requirement of Article III standing is a significant barrier to plaintiffs seeking recovery as a result of a data breach.

As data privacy litigation develops, however, the barrier to establishing injury may prove to be less elusive. City attorneys and outside counsel who advise cities regarding how to comply with the multitude of laws that regulate the collection, storage, release, availability, integrity, or destruction of individually identifying information should evaluate the potential liability of cities in the event of a breach or unauthorized disclosure or due to the failure to comply with notification requirements, mitigate harm, or implement privacy and security policies and procedures. While there are a number of federal and state laws that impose data privacy requirements on cities, city attorneys and outside counsel should advise clients to initially focus any efforts to ensure compliance on the laws and regulations that have the potential to impose the greatest liability. Admittedly, this is a moving target that shifts on the sands of the readiness of a city's information technology infrastructure and employees, the state of data privacy litigation, and whether lawmakers authorize individuals to seek remedy against public entities. Based on personal experience, however, a city that violates a data privacy or security requirement can minimize - and even avoid - civil penalties if it demonstrates that it is in the process of making a good faith effort to comply with data privacy requirements.

[133] *Id.*

APPENDIX

SUMMARY OF THE IDENTITY THEFT ENFORCEMENT AND PROTECTION ACT AND RELATED STATUTES

State Statutes: Tex. Bus. & Com. Code § 521.002 and 521.053; Tex. Loc. Gov't Code § 205.010(b); Tex. Gov't Code § 2054.1125(b).	
Sensitive Personal Information Definition	The statute applies to "Sensitive Personal Information", which includes an individual's first name or first initial and last name in combination with any one or more of the following, if the information is not encrypted: • Social Security number; • Driver's license number or government-issued identification number; and • Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's account. In addition, SPI is information that identifies an individual and relates to: • The physical or mental health or condition of the individual; • The provision of health care to the individual; or • Payment for the provision of health care to the individual.
Persons Covered	A business, local government or state agency that conducts business in Texas and owns, licenses or maintains computerized data that includes sensitive personal information.
Standard for Triggering	The statute is triggered upon discovery or the receipt of notification of a breach of system security. "Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key to decrypt the data.
Specific Notice Content Requirements	Not specified in statute.
Time to Notify Affected Persons of Breach	Disclosure should be made as quickly as possible or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. However, disclosure may be delayed at the request of law enforcement agency that determines that the notification will impede a criminal investigation. Any person who maintains computerized data that includes sensitive personal information not owned by the person must notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Exemptions	Sensitive personal information only includes data items that are not encrypted unless the encryption key is also breached.

Penalty	The Attorney General may bring a civil suit for damages or an injunction. A person who violates the statute is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. A person who fails to take reasonable action to comply with notification requirements is liable to the state for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day the person fails to take reasonable action to notify with a maximum penalty of $250,000 for a single breach. If it appears to the Attorney General that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the Attorney General may bring an action in the name of the State against the person for a temporary restraining order or by a permanent or temporary injunction. These provisions do apply to a local government.
Private Right of Action	A violation of this statute is also a deceptive trade practice under the Texas Deceptive Trade Practices Act; however, the Texas Deceptive Trade Practices Act does not apply to a local government.
Other Provisions	Affected individuals residing in states with no data breach notification statutes (currently: Alabama, New Mexico, and South Dakota) must be notified in accordance with Texas law. If an entity must notify over 10,000 individuals of a breach, the entity must notify each consumer reporting agency of the timing, distribution, and content of the notices without unreasonable delay. A business must implement and maintain reasonable procedures, including appropriate corrective action, to protect from unlawful use or disclosure of sensitive personal information, such as shredding, erasing, or other similar means of modifying sensitive personal information to make it unreadable or indecipherable. This provision does not apply to a local government.

SUMMARY OF THE TEXAS MEDICAL RECORDS PRIVACY ACT AND RELATED STATE LAWS, FEDERAL LAWS, AND REGULATIONS

State and Federal Statutes and Regulations: Tex. Health & Safety Code, Chapter 181; Tex. Loc. Gov't Code § 205.010(b); Tex. Bus. & Com. Code § 521.002 and 521.053.	
Protected Health Information Definition	Protected health information ("PHI") is not defined in the Texas Medical Records Privacy Act (the "TMRPA") but TMRPA incorporates the definition of PHI under the Health Insurance Portability and Affordability Act ("HIPAA") and the Privacy Standards. Thus, for purposes of TMRPA, PHI means: • Individually identifiable health information transmitted or maintained in any form or medium by a covered entity or its business associate; or • Health information (including demographic information) that relates to an individual's physical health, mental health, the provision of health care, or health care payment that identifies the individual. PHI does not include: (i) Family Educational Rights and Privacy Act (FERPA) or (ii) Employment records unless the records are electronically transferred. For a local government, "Sensitive personal information" has the meaning assigned by the ITEPA. In addition, the breach of PHI by a covered entity that is a governmental unit triggers the notice requirements under the ITEPA. Individually Identifiable Health Information means information that is collected from an individual, including demographic information that either identifies the individual or can be used to identify the individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to either: • The past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or • The past, present, or future payment for the provision of health care to an individual.
Persons Covered	TMRPA applies to a "Covered Entity", which is defined as any person who for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis: (i) engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting PHI; (ii) comes into possession of PHI; (iii) obtains or stores PHI under TMRPA; or (iv) is an employee, agent, or contractor of a covered entity insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits PHI. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or a person who maintains an Internet site.

Standard for Triggering	TMRPA does not include any breach notification requirements. A local government that is a TMRPA covered entity and experiences a breach incident must comply with breach notification requirements if the entity owns, licenses, or maintains computerized data that includes SPI and the breach compromises the security, confidentiality, or integrity of the information. Under the ITEPA, "breach of system security" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of SPI maintained by a local government, including data that is encrypted if the person who acquires the data has the key to decrypt the data. Such a breach triggers the notice requirements under the ITEPA. The ITEPA is triggered upon discovery or the receipt of notification of a breach of system security.
Specific Notice Content Requirements	Not specified in statute.
Time to Notify Affected Persons of Breach	TMRPA incorporates HIPAA's definition of PHI. The definition of SPI under TMRPA is very similar to the definition of PHI under HIPAA. Therefore, the breach of PHI by a TMRPA covered entity triggers the notice requirements under the ITEPA. Thus, disclosure to the affected persons(s) should be made as quickly as possible or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. However, disclosure may be delayed at the request of a law enforcement agency if the agency determines that the notification will impede a criminal investigation.
Exemptions	Partial Exemption for Records of Employer: Except for regulations regarding the re-identification of PHI, marketing of PHI, sale of PHI, and the electronic disclosure of PHI, TMRPA does not apply to PHI held by an employer. Workers' Compensation: TMRPA does not apply to workers' compensation insurance, a function authorized by Title 5 of the Labor Code, or any person in connection with providing, administering, supporting, or coordinating any of the benefits under a workers' compensation self-insured program. Employee Benefit Plans: TMRPA does not apply to an employee benefit plan, a covered entity or person acting in connection with an employee benefit plan. Offenders with Mental Impairments: TMRPA does not apply to an agency listed or described in Health and Safety Code, Section 614.017 that disclosures, receives, transfers, or exchanges the PHI relating to a special needs offender or a juvenile with a mental impairment in the custody of the agency for purposes of continuity of care and services. Among other entities, listed agencies include local jails regulated by the Commission on Jail Standards, a municipal or county health department, a hospital district and a judge with jurisdiction over juvenile or criminal cases. Crime Victim Compensation: TMRPA does not apply to an entity in

	connection with providing, administering, supporting, or coordinating benefits regarding compensation to crime victims as provided by Code of Criminal Procedure, Chapter 56, Subchapter B.
Penalty	The Attorney General may institute an action for civil penalties for violations of TMRPA not to exceed: • $5,000 per violation per year committed negligently, • $25,000 per violation per year if committed knowingly or intentionally, or • $250,000 per violation if the covered entity knowingly or intentionally used the PHI for financial gain. Penalty Reduction: The total amount of a penalty assessed against a covered entity under TMRPA in relation to a violation of the electronic disclosure of PHI is capped at $250,000 annually if the court finds that the disclosure was made to another covered entity for treatment, payment, health care operations, performing an insurance or health maintenance organization function or as otherwise authorized or required by state or federal law and the court finds that: • The PHI disclosed was encrypted or transmitted using encryption technology designed to protect against improper disclosure; • The recipient of the PHI did not use or release the PHI; or • At the time of the disclosure of the PHI, the covered entity had developed, implemented, and maintained security policies, including the education and training of employees responsible for the security of PHI. Mitigation: In a proceeding to impose an administrative or civil penalty due to the disclosure of individually identifiable health information, a covered entity may introduce, as mitigating evidence, evidence of the entity's good faith efforts to comply with: • State law related to the privacy of individually identifiable health information; or • HIPAA and Privacy Standards. In determining a penalty imposed on a covered entity that is licensed by a state agency, a court or state agency must consider these factors: • The seriousness of the violation, including the nature, circumstances, extent, and gravity of the disclosure; • The covered entity's compliance history; • Whether the violation poses a significant risk of financial, reputational, or other harm to an individual whose PHI is involved in the violation; • Whether the covered entity was certified at the time of the violation under Health & Safety Code, Section 182.108; • The amount necessary to deter a future violation; and • The covered entity's efforts to correct the violation.
Private Right of Action	A violation of this statute is also a deceptive trade practice under the Texas Deceptive Trade Practices Act; however, the Texas Deceptive Trade Practices Act does not apply to a local government.

Other Provisions	Electronic Disclosure of PHI: A covered entity may not electronically disclose an individual's PHI without a separate authorization from the individual or the individual's legally authorized representative for each disclosure. The authorization is not required if the disclosure is authorized or required by state or federal law. A covered entity may provide general notice by: • Posting a written notice in the covered entity's place of business; • Posting a notice on the covered entity's Internet website; or • Posting a notice in any other place where individuals whose PHI is subject to electronic disclosure are likely to see the notice. Training: Each covered entity must train its employees on state and federal laws regarding PHI within 90 days after the employee is hired and within one year of a material change in law concerning PHI. Each employee must sign a statement verifying the employee's training. The covered entity must maintain these signed statements for six years. Sale of PHI: A covered entity may not disclose an individual's PHI to anyone in exchange for direct or indirect remuneration. Marketing Using PHI: PHI may not be used or disclosed for marketing purposes without first obtaining consent or authorization from the individual. Written communications must explain the recipient's right to removal from the mailing list, and removal must be accomplished within 45 days after the receipt of the request. Re-identification of PHI: A covered entity may not re-identify or attempt to re-identify PHI to identify an individual unless the individual provides prior consent or authorization. The Privacy Standards: TMRPA adopts the Privacy related to an individual's right to access to his/her PHI and ability to amend his/her PHI.

SAMPLE GENERAL NOTICE THAT PROTECTED HEALTH INFORMATION IS SUBJECT TO ELECTRONIC DISCLOSURE

Notice that Protected Health Information is Subject to Electronic Disclosure

*****

Your medical and medical billing information is subject to electronic disclosure by the City of _____.

*****

The City is restricted from disclosing your medical or medical billing information ("protected health information"), in electronic format unless it provides notice and receives authorization from you or your legally authorized representative to disclose this information.

Under the Texas Medical Records Privacy Act, the City must obtain your authorization to electronically disclose your protected health information unless it is disclosed for certain purposes or as required by law. The City may electronically disclose your protected health information without your authorization to any person outside of the City if the disclosure is: authorized or required by law; for the purpose of treatment, payment or health care operations; to another covered entity; to perform an insurance or health maintenance organization function described by Section 602.053 of the Insurance Code; or as required by state or federal law. Any other electronic disclosure of your protected health information requires the City to obtain an authorization from you or your legally authorized representative.

An authorization for disclosure under the Texas Medical Records Privacy Act may be made in writing, electronic form or in oral form if oral authorization is documented in writing by the City. For more information about your rights under the Texas Medical Records Privacy Act, visit https://www.texasattorneygeneral.gov/cpd/state-and-federal-health-privacy-laws or call the Texas Attorney General's Consumer Protection Hotline: (800) 621-0508.

AGREEMENT FOR
RELEASE OF DRIVER RECORDS
TO GOVERNMENTAL ENTITIES

This document constitutes an ("Agreement") made between the Texas Department of Public Safety ("TXDPS"), which is the state administrator for driver license and identification card records, and the Governmental Entity identified below ("the Governmental Entity"), which shall be referred to herein as "the Parties."

Governmental Entity Name: _____

Address: _____

WHEREAS, Texas law authorizes TXDPS to provide Driver Records individually and in bulk for specified permissible purposes;

WHEREAS, Texas law authorizes TXDPS to establish an Interactive System to provide the release of Driver Records;

WHEREAS, state and federal law, including the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. §2721 *et seq.*) and the Texas Motor Vehicle Records Disclosure Act (Chapter 730 of the Texas Transportation Code) extend privacy protections to Personal Information maintained in the files of state motor vehicle agencies such as TXDPS;

WHEREAS, the Governmental Entity desires to obtain Driver Records, including Personal Information, from TXDPS; and

WHEREAS, Texas law requires each prospective Governmental Entity to execute a written agreement or contract containing safeguards TXDPS considers necessary or reasonable to ensure that Driver Records obtained are used only for permissible purposes and that the rights of individuals and TXDPS are protected before the Governmental Entity receives any Driver Records.

THEREFORE, IT IS AGREED, that TXDPS shall deliver Driver Records in an electronic format to the Governmental Entity, subject to the following terms and conditions:

1. **Definitions:**
   a. **Driver Records** means a record that pertains to a motor vehicle operator or driver license or permit, or identification document issued by TXDPS. It includes the following types of records: Type 1 (status record); Type 2 (a 3-year driving history record); Type 3 (a list of all crashes and violations in the record for commercial drivers only); and Type 4 (school bus driver records).

   b. **Interactive System** means the process by which TXDPS supplies Driver Records in an electronic format, including real-time and batch web-based applications.

c. Personal Information means information that identifies an individual, including but not limited to an individual's date of birth, driver license number or identification card number, name, and address.

2. Certification of Permissible Use(s):

The Governmental Entity, by signing this Agreement, hereby certifies compliance with all provisions of the federal Driver's Privacy Protection Act of 1994, the Texas Motor Vehicle Records Disclosure Act, and with all other state and federal laws applicable to this Agreement. The Governmental Entity certifies that its use of Driver Records obtained under this Agreement is for the following permissible purpose(s) only and for no others:

Initial all that apply.

_____ 1. For use in connection with any matter of: (a) motor vehicle or motor vehicle operator safety; (b) motor vehicle theft; (c) motor vehicle emissions; (d) motor vehicle product alterations, recalls, or advisories; (e) performance monitoring of motor vehicles or motor vehicle dealers by a motor vehicle manufacturer; (f) removal of nonowner records from the original owner records of a motor vehicle manufacturer to carry out the purposes of: the Automobile Information Disclosure Act, 15 U.S.C. Section 1231 *et seq.*; 49 U.S.C. Chapters 301, 305, 323, 325, 327, 329, and 331; the Anti Car Theft Act of 1992, 18 U.S.C. Sections 553, 981, 982, 2119, 2312, 2313, and 2322, 19 U.S.C. Sections 1646b and 1646c, and 42 U.S.C. Section 3750a *et seq*., all as amended; the Clean Air Act, 42 U.S.C. Section 7401 *et seq*., as amended; and any other statute or regulation enacted or adopted under or in relation to a law included in this subsection; (g) child support enforcement under Chapter 231, Family Code; or (h) enforcement by the Texas Workforce Commission under Title 4, Labor Code.

_____ 2. For use by a government agency, including any court or law enforcement agency, in carrying out its functions or a private person or entity acting on behalf of a government agency in carrying out the functions of the agency.

_____ 3. For use in connection with a matter of: (a) motor vehicle or motor vehicle operator safety; (b) motor vehicle theft; (c) motor vehicle product alterations, recalls, or advisories; (d) performance monitoring of motor vehicles, motor vehicle parts, or motor vehicle dealers; (e) motor vehicle market research activities, including survey research; or (f) removal of nonowner records from the original owner records of motor vehicle manufacturers.

_____ 4. For use in the normal course of business by a legitimate business or an authorized agent of the business, but only to verify the accuracy of Personal Information submitted by the individual to the business or the authorized agent of the business; and, if the information is not correct, to obtain the correct information for the sole

purpose of preventing fraud by pursuing a legal remedy against or recovering on a debt or security interest against the individual.

_____ 5. For use in conjunction with a civil, criminal, administrative, or arbitral proceeding in any court or government agency or before any self-regulatory body, including service of process, investigation in anticipation of litigation, execution or enforcement of a judgment or order, or under an order of any court.

_____ 6. For use in research or in producing statistical reports, but only if the Personal Information is not published, redisclosed, or used to contact any individual.

_____ 7. For use by an insurer or insurance support organization, or by a self insured entity, or an authorized agency of the entity in connection with claims investigation activities, antifraud activities, rating, or underwriting.

_____ 8. For use in providing notice to an owner of a towed or impounded vehicle.

_____ 9. For use by a licensed private investigator agency or licensed security service for a purpose permitted as stated herein.

_____ 10. For use by an employer or an authorized agent or insurer of the employer to obtain or verify information relating to a holder of a commercial driver's license that is required under 49 U.S.C. Chapter 313.

_____ 11. For use in connection with the operation of a private toll transportation facility.

_____ 12. For use by a consumer reporting agency, as defined by the Fair Credit Reporting Act (15 U.S.C. §1681 *et seq*.), for a purpose permitted under that Act.

_____ 13. For use in the prevention, detection, or protection against personal identity theft or other acts of fraud. Prior to release of Personal Information, TXDPS may require additional information.

_____ 14. For any other purpose specifically authorized by law that relates to the operation of a motor vehicle or to public safety. Please provide the statutory authority:

Texas Transportation Code 521.022 subsection (d)

The Governmental Entity shall restrict access to, use of, and disclosure of Driver Records, including Personal Information, to designated personnel solely for the purposes as identified herein. Access to and use of Driver Records by the Government Entity's personnel that are not authorized is strictly prohibited. Any access, use and disclosure not required for the purposes of this Agreement or for any unofficial purpose is strictly prohibited. Violation of the federal Driver's Privacy Protection Act or the Texas Motor Vehicle Records Disclosure Act may result in civil and criminal penalties.

3. Resell or Redisclosure:
The Governmental Entity shall not resell or redisclose Personal Information obtained under this Agreement to third parties in the identical or a substantially identical format. The Governmental Entity may resell or redisclose Personal Information only for a use authorized by Texas Transportation Code, Section 730.007, and in compliance with the sections herein entitled "Record Creation and Retention" and "Provide Copies of Records and Notification of Release." Personal Information under the Driver's Privacy Protection Act and the Texas Motor Vehicle Records Disclosure Act is not subject to the Texas Public Information Act.

4. Record Creation and Retention:
If the Governmental Entity legally resells or rediscloses Personal Information obtained from Driver Records under this Agreement, the Governmental Entity shall create a record identifying each person or entity that obtained Personal Information from the Governmental Entity and the legally permissible purpose for which Driver Records were obtained. The Governmental Entity shall ensure that any third party to which it releases any Driver Records shall comply with all federal and state laws on the release of the information and all terms, conditions, and obligations of this Agreement. The Governmental Entity shall retain such records for a period of not less than five (5) years following transfer of Driver Records to the third party of the following: the name of any person or entity to whom the release was made; the date the release was made; the permitted use for which Driver Records were released; the written agreement with the third party; and contact information for the person or entity Driver Records were released to.

5. Provide Copies of Records and Notification of Release:
If the Governmental Entity rediscloses any Driver Records obtained under this Agreement to a third party, the Governmental Entity shall provide access to or copies of those records required in the section herein entitled "Record Creation and Retention" to TXDPS immediately upon TXDPS' request. TXDPS retains the right to require the records in any applicable format, including electronic or paper. The Governmental Entity shall bear the expense of providing this information to TXDPS, including any postage or shipping charges.

6. Unauthorized Disclosure:
The Governmental Entity shall immediately, but no later than two (2) calendar days, notify TXDPS of any inadvertent or unauthorized release, disclosure, breach, or compromise of Driver Records obtained under this Agreement as soon as the Governmental Entity knows or should have known of such unauthorized or inadvertent release, disclosure, breach, or compromise of security. This obligation applies whether the action or omission was by the Governmental Entity, its employees or agents, or by any person or entity that acquired Driver Records from the Governmental Entity, either directly or indirectly. The Governmental Entity shall notify TXDPS of any breach of system security as required by Section 521.053(c) of the Texas Business and Commerce Code, and shall cooperate fully with TXDPS in any investigation thereof.

7. Fees:
Pursuant to Texas Transportation Code Section 521.049, TXDPS shall not charge a fee for Driver Records disclosed to a law enforcement or other governmental agency for an official

purpose, unless the Governmental Entity requests Driver Records sold in bulk for research purposes. A Governmental Entity obtaining Driver Records for research shall enter into a separate contract with TXDPS to purchase Driver Records for a fee.

8. Acknowledgement and Disclaimer:
The Governmental Entity acknowledges that TXDPS is furnishing Driver Records on an "as is" basis and TXDPS makes no representation or warranty as to the accuracy of any Driver Records furnished. TXDPS expressly disclaims responsibility for any failure to deliver Driver Records in a timely manner, or at all, in the event of staff shortages, failures of appropriations, breakdown of equipment, compliance with new or amended laws, acts of authority exercised by a public official, acts of God, or other circumstances which may delay or preclude furnishing Driver Records in a timely fashion. If Driver Records are not furnished, TXDPS has no further responsibility or liability to the Governmental Entity with respect to undelivered Driver Records and has no liability or responsibility whatsoever for delayed Driver Records.

9. Consumer Protection:
Driver Records furnished under this Agreement shall not be used by the Governmental Entity to engage in any method, act, or practice that is unfair or deceptive, nor shall Driver Records be used for marketing, solicitations, or surveys not authorized by law.

10. Direct Access to Driver Records:
No member of the public or any person outside the direct employ or control of the Governmental Entity shall be permitted direct access to Driver Records through the Governmental Entity under this Agreement for any reason other than the Governmental Entity's intended and legitimate use of Driver Records.

11. Assignability:
The Governmental Entity shall not assign, license, or transfer any of its rights, duties, and obligations under this Agreement without the prior written consent of TXDPS. An attempted assignment in violation of this section is null and void. Any approved assignment shall not relieve the assignor of any liability or obligation under this Agreement.

12. Successors:
This Agreement shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors, heirs, administrators, personal representatives, legal representatives, and permitted assigns.

13. Incorporation of Other Documents:
This Agreement, including "Attachment A, Governmental Entity Information Form," constitutes the entire agreement between the Parties with regard to the matters made the subject of this Agreement. There are no verbal representations, inducements, agreements, understandings, representations, warranties, or restrictions between the Parties other than those specifically set forth herein.

14. Interactive System for Driver Records:
The Interactive System for Driver Records, by which TXDPS supplies Driver Records in an electronic format including real-time and batch web-based applications, is operated and controlled by a State of Texas Vendor. The State of Texas Vendor is the duly authorized service agent of TXDPS responsible for processing electronically submitted Driver Records requests and delivering Driver Records in a secure, electronic format utilizing the Interactive System. The State of Texas Vendor is obligated to specific performance level requirements. As such, the State of Texas Vendor has the authority to suspend any Governmental Entity account or access to the Interactive System when such access compromises the operation of the Interactive System. Suspension of such account or access shall continue until the compromising condition is resolved to the satisfaction of TXDPS.

15. Term of Agreement:
The term of this Agreement shall begin on the date it is signed by the last of the two Parties to this Agreement and shall continue in full force and effect for a term of three (3) years. Upon an amendment in writing to this Agreement executed by both Parties, this Agreement may be renewed for intervals of three (3) year at a time.

16. Termination:

a. For Convenience: Either Party may terminate this Agreement for convenience at any time for any reason by giving the other Party thirty (30) calendar days written notice. If a Party elects to terminate this Agreement for convenience, all unfilled obligations shall remain in full force. In no event will termination for convenience by TXDPS give rise to any liability whatsoever on the part of TXDPS.

b. For Cause: TXDPS may immediately terminate this Agreement for cause for any violation of the terms of this Agreement or for any violation of any state or federal law or regulation relating to the subject matter of this Agreement. TXDPS shall provide the Governmental Entity with written notice to terminate this Agreement, which termination shall become effective immediately upon Governmental Entity's receipt of the notice. If this Agreement is terminated for cause, TXDPS may refuse to provide Driver Records to the Governmental Entity in any format.

c. Mutual Termination: This Agreement may further be terminated by mutual agreement and consent, in writing, by both Parties.

17. Change of Status:
This Agreement shall automatically terminate if the Governmental Entity ceases to exist, substantially changes the nature of its governing business, or if it ceases to qualify for Driver Records under the permissible use(s) certified in the section herein entitled "Certification of Permissible Use(s)." The Governmental Entity shall immediately notify TXDPS in writing of any change in status that may implicate this section.

18. Amendments:
TXDPS may amend the terms and conditions of this Agreement from time to time in order to accommodate changes in the records or information furnished under this Agreement and for other reasons deemed appropriate by TXDPS. No modification or amendment to this Agreement shall become valid unless in writing and signed by both Parties. All correspondence regarding modifications or amendments to this Agreement shall be forwarded to TXDPS for prior review and written approval. Only an authorized representative or an authorized designee shall be authorized to sign changes or amendments.

19. Notice:
Any notice required or permitted under this Agreement shall be directed to the Parties at the addresses shown below. The following contact person(s) is designated by the Governmental Entity to receive all notices regarding this Agreement:

Point of Contact: _____

Alternate Point of Contact: _____

Address: _____

City, State, Zip Code: _____

Telephone Number: _____

Cell Phone Number: _____

Fax: _____

Email: _____

All correspondence to TXDPS regarding this Agreement shall be mailed to the following address:

Texas Department of Public Safety
License and Record Service/Online Services
P.O. Box 4087
Austin, Texas 78773-0360
(512) 424-5967
Fax: (512) 424-7456
Email: e.Commerce@dps.texas.gov

Notices to the Parties at the addresses shown above shall be deemed received: (i) when delivered in hand and a receipt granted; (ii) three (3) calendar days after it is deposited in the United States mail by certified mail, return receipt requested; or (iii) when received if sent by confirmed

facsimile or confirmed email. Either of the Parties may change its address or designated individual(s) to receive notices by giving the other Party written notice as provided above, specifying the new address and/or individual and the date upon which it shall become effective.

20. No Joint Enterprise:
TXDPS is associated with the Governmental Entity only for the purposes and to the extent set forth herein. The Governmental Entity is an independent entity and shall have the sole right to supervise, manage, operate, control, and direct the performance of the details incident to its duties hereunder. Nothing contained herein shall be deemed or construed to create a partnership or joint venture, to create the relationship of an employer-employee or principal-agent, or to otherwise create any liability for whatsoever with respect to the indebtedness, liabilities, and obligations of the Governmental Entity or any other party.

21. No Liability for Employees and Officers:
Each Party to this Agreement shall have no liability whatsoever for the actions or omissions of an individual employed or contracted by another Party, regardless of where the individual's action or omissions occurred. Each Party is solely responsible for the actions or omissions of its employees and agents; however, such responsibility is only to the extent required by Texas law. Where injury or property damage results from the joint or concurring acts or omissions of the Parties, liability, if any, shall be shared by each party in accordance with the applicable laws of the State of Texas, and subject to all defenses, including governmental immunity. These provisions are solely for the benefit of the Parties hereto and not for the benefit of any person or entity not a Party hereto; nor shall any provision hereof be deemed a waiver of any defenses available by law.

22. Compliance with Law:
The Parties shall comply with all local, state, and federal laws and regulations applicable to the subject matter of this Agreement, including but not limited to, the federal Driver's Privacy Protection Act of 1994 and the Texas Motor Vehicle Records Disclosure Act.

23. Interpretation Against the Drafter:
Regardless of which Party drafted this Agreement or the language at issue, any ambiguities in this Agreement or the language at issue shall not be interpreted against the drafting Party.

24. Non-Waiver:
Any failure of TXDPS, at any time, to enforce or require the strict keeping of any provision of this Agreement shall not constitute a waiver of such provision, and shall not affect or impair same or the right of TXDPS at any time to avail itself of same.

25. Headings:
The headings, captions, and arrangements used in this Agreement are for convenience only and shall not be deemed to limit, amplify, modify, or to affect the meaning of the terms of this Agreement.

26. Severability:
If one or more provisions of this Agreement or the application of any provision to any Party or circumstance is held invalid, unenforceable, or illegal in any respect by a final order/judgment of the State Office of Administrative Hearings or a court of competent jurisdiction, the remainder of this Agreement and the application of the provision to other parties or circumstances shall remain valid and in full force and effect.

27. Audit and Inspection:
The Governmental Entity is subject to audit and inspection, at any time during normal business hours and at a mutually agreed upon location, by the State Auditor, TXDPS, and any other department or agency responsible for determining that the Parties have complied with applicable law. The Governmental Entity shall provide all reasonable facilities and assistance for the safe and convenient performance of any audit or inspection. The Governmental Entity shall keep all records and documents regarding this Agreement for the term of this Agreement and for five (5) years after the termination of this Agreement.

28. Governing Law and Jurisdiction:
This Agreement shall be construed in accordance with the laws of the State of Texas. Except as otherwise provided by Chapter 2260 of the Texas Government Code, venue for any litigation shall be Travis County, Texas.

29. Chapter 2260, Texas Government Code:
The Governmental Entity shall use the dispute resolution process provided for in Chapter 2260 of the Texas Government Code and the applicable TXDPS administrative rules to attempt to resolve all disputes or contract claims arising under this Agreement.

30. Survival:
Any provisions of this Agreement that impose continuing obligations on the Parties, including but not limited to the following, shall survive the expiration or termination of this Agreement for any reason: confidentiality and security obligations; notice regarding any unauthorized disclosure or breach; resell or redisclosure obligations; audit obligations; and any other provision that imposes a continuing obligation on the Governmental Entity.

31. Signature Authority:
The signatory for the Governmental Entity hereby represents and warrants that it has full and complete authority to execute this Agreement.

32. Certifications:
The Parties certify the following: (i) each Party paying for the performance of governmental functions or services must make those payments from current revenues available to the paying Party; (ii) this Agreement is authorized by the governing body of the Parties; (iii) each Party has the authority to enter into this Contract by authority granted in Texas Transportation Code, Chapter 521 and 730; (iv) the services specified above are necessary and essential for activities that are properly within the statutory functions and programs of the affected agencies; (v) the

proposed arrangement serves the interest of efficient and economical administration of government; and (vi) the services, supplies or materials contracted for are not required by Section 21 of Article 16 of the Texas Constitution to be supplied under contract given to the lowest responsible bidder.

IN WITNESS WHEREOF, the Parties have executed this Agreement on the date written below.

DEPARTMENT OF PUBLIC SAFETY:	**GOVERNMENTAL ENTITY:**
_____	_____
Signature	Signature
_____	_____
Name and Title	Name and Title
_____	_____
Date	Date

ATTACHMENT A
GOVERNMENTAL ENTITY INFORMATION FORM

Nature of the Governmental Entity's Activities:

_____

_____

_____

List all URL addresses/Facebook/Twitter accounts used or possessed by the Governmental Entity:

_____

_____

_____

Intended use of Driver Records obtained from TXDPS (Describe how the exemption qualifies for obtaining Driver Records):

_____

_____

_____

_____

_____

_____

If the Governmental Entity intends to release Driver Records obtained from TXDPS, explain what safeguards and/or assurances are in place to meet the requirements of this Agreement:

_____

_____

_____

If the Governmental Entity does not intend to release Driver Records to another entity, state so below:

_____

_____

_____

For Department Use Only

STATE OF TEXAS §

COUNTY OF TRAVIS §

Motor Vehicle Inquiry (MVI) Service Contract for Accessing Texas Motor Vehicle Records

THIS CONTRACT, is made by and between the State of Texas, acting by and through the Texas Department of Motor Vehicles, hereinafter called the "State," and

_____,

hereinafter called the "Purchaser."

WITNESSETH

WHEREAS, Texas Transportation Code, Chapter 501, 502, 504 and 520 establish that the State is responsible for administering and retaining Texas motor vehicle title and registration records (MVRs); and

WHEREAS, this contract is made in accordance with the provisions of Texas Transportation Code, Chapter 730, the state Driver's Privacy Protection Act; and

WHEREAS, the State is authorized by Title 43, Texas Administrative Code, §**217.92**, to enter into written service agreements with individuals, businesses, and governmental agencies to provide electronic access to vehicle title and registration information; and

WHEREAS, the Purchaser requests from the State authority to access the Vehicle Title and Registration (VTR) database in order to obtain information from MVRs by remote electronic access through the Internet, via a secure web site; and

WHEREAS, the Federal Drivers Privacy Protection Act (18 U.S.C. §2721 et seq.) and Texas Drivers Privacy Protection Act authorizes the department to disclose personal information contained in the department motor vehicle records only in accordance with the Acts; and

WHEREAS, the State will provide remote electronic access to the Purchaser provided the Purchaser agrees to the terms and conditions of this contract; and

WHEREAS, the **Texas Motor Vehicle Board**, adopted Title 43, Texas Administrative Code, Chapter 217, Subchapter F establishing the costs the State may assess a Purchaser for remote electronic access to the VTR database;

AGREEMENT

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the parties do hereby agree as follows:

The State shall provide the Purchaser remote electronic access, through the Internet, via a secure web site, to the Vehicle Title and Registration (VTR) database, under the following conditions:

1. INFORMATION AVAILABLE

The State will make available, in accordance with the federal and Texas Drivers Privacy Protection Acts (DPPAs) information contained in the MVRs and the VTR database.

2. CERTIFICATION OF USE

The State will release information contained in the MVRs and VTR database only if the Purchaser certifies its intended use of the information in Attachment A to this contract. Certified intended uses include only those uses for which the Purchaser itself will actually employ the information; certified intended uses do not include uses that are speculative or that will be engaged in by persons acquiring the information from the Purchaser.

3. RESTRICTIONS

A. The Purchaser may use information obtained from MVRs and the VTR database only in accordance with the DPPAs and only for the use or uses certified to in Attachment A.

B. The Purchaser shall access the MVRs by license plate number, vehicle identification number, title or document number, or placard number.

C. The Purchaser shall not provide motor vehicle registration information to anyone in response to a telephone inquiry by license plate number.

D. The Purchaser shall utilize the State "data" only for the purposes stated in this contract and none other, and the data reflects notices of transfers of vehicles received by the State. Failure on the Purchaser's part to properly interpret the State data shall be the fault of the Purchaser and liability for sending violation notices to the incorrect party(ies) shall rest with the Purchaser, and not the State. If the data continues to be interpreted improperly, then the contract is subject to termination.

E. **Resale and Redisclosure:** A Purchaser obtaining privacy protected personal information, may only resell or redisclose the privacy protected personal information for a permitted use authorized by law that:
   1. Purchaser has indicated for its own use; or
   2. The Requestor is obtaining as agent of an authorized recipient for the authorized recipient's own user as permitted under Transportation Code, Section 730.007.

All uses must be listed in Attachment A. Information may not be obtained solely for the purpose of resale or redisclosure. An authorized recipient may not redisclose the information in the identical or a substantially identical format received under this contract.

The Purchaser must maintain records of any entity or person that received the information and the permitted use for which it was obtained. These records must be maintained for a period of not less than five (5) years and must be made available to the State for inspection, upon request. Any person or entity obtaining privacy protected information from the Purchaser, directly or indirectly, must

comply fully with the provisions of the DPPAs. Any violation of the above law by a person or entity acquiring privacy protected information from the Purchaser, directly or indirectly, will be considered a breach of this contract by the Purchaser.

The Purchaser shall immediately inform the State if privacy protected personal information provided to the Purchaser is disclosed in violation of the DPPAs. This obligation applies whether the disclosure was by the Purchaser or by a person or entity that acquired privacy protected information from the Purchaser, directly or indirectly. Information may not be obtained solely for the purpose of resale or redisclosure.

4. TERM OF CONTRACT

This contract becomes effective upon agreement and execution by both parties. The contract is subject to a continuous automatic annual renewal unless terminated in accordance with Paragraph 11 of this contract, Termination.

The State reserves the right to amend any of the provisions of the contract or to waive any violations of this contract by the Purchaser.

5. USER IDS

This Motor Vehicle Inquiry Service Contract can be for multiple business location and multiple User IDs, if applicable.

Prior to issuance of any User IDs by the State, a properly executed Request for *External Access to TxDMV Information Systems (Attachment B)* and *Information Security Compliance Agreement (Attachment C)* must be submitted for each person requesting access to MVRs. Each person who, by virtue of this agreement, is allowed access to MVRs from this business location will be assigned a unique User ID to be used only by that person. The user id is not to be shared with anyone. ***After 365 days of nonuse, user id(s) will automatically be deleted.***

6. DEPOSIT:

A deposit of at least $200.00 must be maintained in a **non-interest bearing** escrow account. This initial deposit is to cover estimated service use. Such escrow account will be established by the State prior to the assignment of User IDs which allow access to MVRs. Payment of the deposit shall be made by check or money order, payable to the "Texas Department of Motor Vehicles", or via credit card and is due upon execution of this contract. The minimum balance in the escrow account may increase, depending on established monthly usage by the Purchaser. The Purchaser may deposit additional funds into the escrow account in excess of the stated minimum balance. When it becomes necessary to increase the Purchaser's escrow account minimum balance, as determined by the State, the Purchaser agrees to pay the sum in increments of $200.00. This additional funding is payable within fifteen (15) days from receipt of the State's notification. PLEASE NOTE: Upon refunding this escrow deposit, the State Comptroller may place a hold on these funds if there is outstanding state debt (indebtedness, tax delinquency or student loan default).

7. CHARGES:

A monthly base charge of $23.00, plus $ .12 per vehicle inquiry, will be assessed, as provided for in Title 43, Texas Administrative Code, Chapter 3. These charges may be prepaid and credited to **the non-interest bearing** escrow account at the request of the Purchaser. Service charges will be deducted from the escrow account until the balance of that account reaches the minimum required balance for the Purchaser, as determined by the State and provided herein.

8. PAYMENT

The total amount is due monthly on or before the due date specified in the State's invoice. Invoices are sent out via E-Billing. Any advance or overpayments will be credited to the account and applied to the next billing statement. Any payment schedule must comply with these provisions. Payment methods are as follows:

Mail check or Money Order to:

Texas Department of Motor Vehicles
IT Services Division, Data Support Services
PO Box 12098
Austin, Texas 78711-2098

Credit Card: Call Data Support Services Branch at (512) 465-1468, option 2.

9. SERVICE HOURS AND INFORMATION

A. The service hours for access of MVRs are 24 hours per day, 7 days per week, with the exception of downtime necessary for routine system maintenance or due to unforeseen or unexpected system downtime.

B. Information regarding billings or payments for your account and technical assistance regarding the information provided may be obtained by contacting Data Support Services Branch, at (512) 465-1468 (Monday through Friday, 8:00 AM – 5:00 PM).

C. Customers with questions or complaints concerning personal solicitation or privacy concerns should contact to the Consumer Relations Division, Contact Center at 1-888-368-4689 (Monday through Friday, 8:00 AM to 5:00 PM).

10. DELINQUENT ACCOUNT:

The Purchaser's account becomes delinquent and subject to termination if the total amount due is not received on or before the due date specified in the State's invoice or if payment is returned due to insufficient funds. If a Purchaser's account is terminated due to delinquency, the balance of the escrow deposit will be refunded, minus any outstanding balance due to the State. Re-establishing service for a terminated delinquent account will require execution of a new contract, pay any previous balance owed, a $200 deposit and a non-refundable processing fee of $50.00.

11. TERMINATION

Termination by State or Purchaser. The State or Purchaser may terminate this contract in writing at any time.

Termination for Cause. Without limiting the foregoing, the State may immediately terminate this contract, without notice, for any violation of the terms of this contract or for any violation of any state or federal law relating to the information provided by the State under this contract.

Automatic Termination. This contract will automatically terminate if the Purchaser ceases to conduct business, if the Purchaser substantially changes the nature of its business, if the Purchaser sells its business, if there is a change in the ownership of the Purchaser, or if the Purchaser dies. The Purchaser, its successor in interest, or its personal representative will immediately notify the State in writing of any change in status that would implicate this paragraph. The Purchaser's successor in interest will be eligible to apply for and execute a new contract.

Effect of Termination. If the contract is terminated by the State or Purchaser, the State will cancel all User IDs associated with the Purchaser's account and refund any unused portion of the non-interest bearing escrow account, minus any outstanding balance due to the State.

12. CANCELLATION OF USER ID:

In the event any User ID assigned to the Purchaser's account by the State is no longer needed for any reason, including, but not limited to, termination, death, or separation from the Purchaser's business of the person to whom the User ID was assigned, the Purchaser shall immediately notify the State by submitting Attachment B, of the cancellation of the User ID. Upon receipt, the State will cancel the User ID.

13. COMPLIANCE WITH LAWS

The Purchaser shall comply with all applicable federal, State, and local laws, statutes, codes, ordinances, rules, and regulations, and with the orders and decrees of any court, or administrative bodies, or tribunals in any matter affecting the performance of this contract. By signing this agreement, the Purchaser certifies that he or she will comply with the provisions of the DPPAs, including, but not limited to, limiting usage to the permissible uses under the Acts.

14. AMENDMENTS

Any changes in the terms and conditions of this contract must be enacted by a written amendment, executed by all parties to this contract.

15. LIMITATION OF LIABILITY

The Purchaser shall save harmless the State from any liability which may arise from the Purchaser's remote electronic access to the VTR database, and the State makes no representation or warranty as to use, result, or accuracy of data contained herein.

16. PRIOR CONTRACTS SUPERSEDED

This contract constitutes the sole and only agreement of the parties here to and supersedes any prior understandings and/or written agreements between the State and the Purchaser respecting the subject matter described herein.

17. SIGNATORY AUTHORITY

The undersigned for the Purchaser represents and warrants that he/she is an officer of the organization for which he/she has executed this contract and that he/she has the full and complete authority to enter into this contract on behalf of the Purchaser.

IN TESTIMONY HEREOF, the parties to this contract have caused these presents to be executed in duplicate counterparts.

_____
PURCHASER

BY: _____
Signature

_____
Name and Title

_____
Address

_____
City, State, and Zip Code

_____
Date

( ) Sole Proprietorship _____
Social Security Number or Employer I.D. Number

( ) Partnership _____
Employer I.D. Number or Tax Number

( ) Corporation _____
Employer I.D. Number or Tax Number

THE STATE OF TEXAS

Executed for the Executive Director and approved for the Texas Motor Vehicle Board for the purpose and effect of activating and/or carrying out the orders, and established policies or work programs heretofore approved and authorized by the Texas Motor Vehicle Board.

BY: _____
Signature

Executive Director, Texas Department of Motor Vehicles
Name and Title

_____
Date

*** * * PLEASE KEEP A COPY OF THIS CONTRACT * * ***

ATTACHMENT A
CERTIFICATION OF USE

NOTE: The State may release information contained in the MVR's and the VTR database only if the Purchaser certifies its intended uses of the information in Attachment "A" to this contract. Certified intended uses include only those uses for which the Purchaser itself will actually employ the information. Certified intended uses do not include uses that are speculative or that will be engaged in by persons acquiring the information from the Purchaser.

PLEASE INITIAL (DO NOT CHECK Y) THE INTENDED USE(S) FOR WHICH REMOTE ELECTRONIC ACCESS TO THE VTR DATABASE IS REQUESTED:

PERMITTED USES:

(I) A. For use in connection with any matter of:

____ (1) motor vehicle or motor vehicle operator safety;
____ (2) motor vehicle theft;
____ (3) motor vehicle emissions;
____ (4) motor vehicle product alterations, recalls, or advisories;
____ (5) performance monitoring of motor vehicles or motor vehicle dealers by a motor vehicle manufacturer; or
____ (6) removal of non-owner records from the original owner records of a motor vehicle manufacturer to carry out the purposes of:
  (a) the Automobile Information Disclosure Act, 15 U.S.C. Section 1231 et seq.;
  (b) 49 U.S.C. Chapters 301, 305, 323, 325, 327, 329, and 331;
  (c) the Anti Car Theft Act of 1992, 18 U.S.C. Sections 553, 981, 982, 2119, 2312, 2313, and 2322, 19 U.S.C. Sections 1646b and 1646c, and 42 U.S.C. Section 3750a et seq., all as amended;
  (d) the Clean Air Act, 42 U.S.C. Section 7401 et seq., as amended; and
  (e) any other statute or regulation enacted or adopted under or in relation to a law included in Paragraphs (a)-(d).

B. Use will be strictly limited to use by:

____ (1) a government agency, including any court or law enforcement agency, in carrying out its functions; or
____ (2) a private person or entity acting on behalf of a government agency in carrying out the functions of the agency.

(II) A. Use in connection with a matter of:

____ (1) motor vehicle or motor vehicle operator safety;
____ (2) motor vehicle theft;
____ (3) motor vehicle product alterations, recalls, or advisories;
____ (4) performance monitoring of motor vehicles, motor vehicle parts, or motor vehicle dealers;
____ (5) motor vehicle market research activities, including survey research; or
____ (6) removal of non-owner records from the original owner records of motor vehicle manufacturers;

B. Use in the normal course of business by a legitimate business or an agent, employee, or contractor of the business, but only:

____ (1) to verify the accuracy of personal information submitted by the individual to the business or an agent, employee, or contractor of the business; and
____ (2) if the information as submitted is not correct or is no longer correct, to obtain the correct information, for the sole purpose of preventing fraud by, pursuing a legal remedy against, or recovering on a debt or security interest against the individual;

C. Use in conjunction:

____ With a civil, criminal, administrative, or arbitral proceeding in any court or government agency or before any self-regulatory body, including service of process, investigation in anticipation of litigation, execution or enforcement of a judgment or order, or under an order of any court;

D. Use in:

____ Research or in producing statistical reports, but only if the personal information is not published, redisclosed, or used to contact any individual;

E. Use by:
____ An insurer or insurance support organization, or by a self-insured entity, or an agent, employee, or contractor of the entity, in connection with claims investigation activities, antifraud activities, rating, or underwriting;

F. Use in:
____ providing notice to an owner of a towed or impounded vehicle;

G. Use by:
____ A licensed private investigator agency or licensed security service for a purpose permitted under this section;

H. Use by:
____ An employer or an agent or insurer of the employer to obtain or verify information relating to a holder of a commercial driver's license that is required under 49 U.S.C. Chapter 313;

I. Use in:
____ Connection with the operation of a private toll transportation facility;

CERTIFICATION

I, _____, the Purchaser, do hereby certify that the intended use of the VTR database information is requested for the permitted use(s) initialed above.

_____
(THE PURCHASER)

BY: _____
(Signature)

_____
(Name and Title)

_____
(Date)

TxDMV
Form 1980
(Rev.02/16)
Page 1 of 1

Attachment B
Request for External Access
To TxDMV Information Systems

Requesting Organization: _____ Date: _____

Account Number/User Id: _____

Please Check One: Add ☐ Change ☐ Delete ☐

Employee Name: _____
Last First MI

Employee Signature: _____

Approved By: _____ _____
Security Administrator (Printed Name and Signature) Phone

For TxDMV Use Only

Describe the information you need to access:

Motor Vehicle Information

Describe the business need for the information and how the information will be used:

Refer to Attachment A

Date_____ Completed By_____

Comments:

TxDMV
Form 1828c
(Rev. 02/16)
Page 1 of 1

Information Resources Security Compliance and Confidentiality Agreement
(VTR External User)

I understand that the Texas Department of Motor Vehicles ("TxDMV") collects and maintains confidential and privileged information and permits access to data containing confidential and privileged information by contractual agreement with external users not employed by TxDMV.

I understand and agree that I will observe the standards of confidentiality that must be maintained as I exchange business and technical information and that unauthorized release of confidential information, or actions deemed negligent resulting in damages/loss of information resources[1], will result in termination of my contract and may also result in legal action.

I understand and agree that any and all information system password(s) or access procedure(s) I receive or devise for use with TxDMV's information systems are confidential and reserved for official state agency business only. I will not disclose to any unauthorized person(s)[2] any password(s) or access procedure(s) I am given or devise, and I will not post these procedure(s) or written password(s) where persons who are not authorized to use TxDMV's system may view them. Attempts to access and utilize TxDMV's information systems for other than their intended purposes may result in prosecution under the Computer Fraud and Abuse Act of 1986 as well as any other applicable statutes and regulations.

I understand and agree that I am responsible for all information system transactions performed as a result of access authorized by the use of my password(s) or procedure(s).

I agree **not** to attempt to circumvent information system security devices or procedures by using or attempting to use any transaction, software, files, or other resources that I am not authorized to use.

I understand that intentionally failing to observe these requirements or intentionally bypassing them may constitute a breach of information systems security as defined in the Texas Penal Code §33.02 and may result in immediate loss of information system access.

I agree to abide by all TxDMV information security policies, procedures, and practices as outlined in the *External TxDMV User Policies*, which are located at ftp://ftp.dot.state.tx.us/pub/txdot-info/isd/external_txdot_user_policies.doc

I acknowledge receipt of this agreement, understand its contents, and agree to abide by the terms set forth herein. Additionally, I have been informed that questions regarding this agreement and/or issues related to the release or disclosure of confidential information should be directed to the director of the TxDMV's Administrative Services Division.

Signature	**Date**
Printed Name	

[1] Information resources include computer systems, telephone systems, voicemail systems, fax systems, and regular mail systems as well as the procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

[2] Unauthorized person(s) include anyone who is not bound by a written confidentiality agreement.

The Texas Department of Motor Vehicles maintains the information collected through this form. With few exceptions, you are entitled on request to be informed about the information that we collect about you. Under §§552.021 and 552.023 of the Texas Government Code, you also are entitled to receive and review the information. Under §559.004 of the Government Code, you are also entitled to have us correct information about you that is incorrect.