ID Safety
Protecting the *real* you, and *only* you.

In partnership with: INTERNATIONAL ASSOCIATION of CHIEFS OF POLICE Bank of America

TEXAS
IDENTITY THEFT RANKING BY STATE: Rank 4, 107.9 Complaints Per 100,000 Population, 25796 Complaints (2007)
Updated January 3, 2009

Current Laws:

Identity Crime: A person commits the offense of fraudulent use or possession of identifying information if he, with the intent to harm or defraud another, obtains, possesses, transfers, or uses the identifying information of (1) another person without the other person's consent; (2) a child younger than 18 years of age; or a deceased person, including a stillborn infant.

Offenses are punished based on the amount of identifying information fraudulently used or possessed. It is a state jail felony if the number of items obtained, possessed, transferred or used is less than five; a felony of the third degree if the number is five to nine; a felony of the second degree if the number is ten to 49; and a felony of the first degree if 50 or more.

Identifying information is defined as information that "alone or in conjunction with other information identifies an individual," including:

- Name, Social Security number, date of birth, mother's maiden name, or government-issued identification number;
- Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
- Unique electronic identification number, address, and routing code, financial institution account number; and
- Telecommunication identifying information or access device.

Statute: Penal Code §32.51:
http://www.statutes.legis.state.tx.us/SOTWDocs/PE/htm/PE.32.htm#32.51

In addition, it is a civil offense for a person to obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name. Violators are liable to the state for a civil penalty of at least $2000 but not more than $50,000 for each violation. The attorney general may bring suit to recover the civil penalty. In addition, if the attorney general believes that a person is engaging or has engaged in identity theft crime, he may bring an action against the person to restrain the violation by a temporary restraining order or temporary or permanent injunction. The attorney general is entitled to recover reasonable expenses incurred in obtaining injunctive relief, civil penalties, or both, under this section, including reasonable attorney's fees, court costs, and investigatory costs.
Statute: Business & Commerce Code §48.101:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.48.htm#48.101

Jurisdiction: State law allows identity theft to be prosecuted in any county in which the offense was committed or in the home county of the victim.
Statute: Code of Criminal Procedure: §13.29:
http://www.statutes.legis.state.tx.us/SOTWDocs/CR/htm/CR.13.htm#13.29

Statute of Limitations: The statute of limitations for identity theft crime is seven years.
Statute: Code of Criminal Procedure: §12.01
http://www.statutes.legis.state.tx.us/SOTWDocs/CR/htm/CR.12.htm#12.01

Phishing: State law prohibits phishing, the act of sending an e-mail that falsely claims to be from an established legitimate enterprise to scam the recipient into surrendering private information, either directly by reply or by sending the recipient to a bogus Web site that looks like the site of the established legal enterprise. The scammer then uses that information for identity crime. The law prohibits a person from creating a web page or domain name without the express authority of the registered owner of the business to induce, request or solicit another person to provide identifying information. Internet service providers and owners of websites or trademarks affected by the phishing scan can file suit against the phishers to seek up to $100,000 for each violation or actual damages, whichever is greater. Punitive damages are available for repeat offenders. There is no private course of action for individuals.
Statute: Business & Commerce: §48.001 through 005:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.48.htm#B

Payment Cards: A person commits an state jail felony, punishable by 180 days to two years in state jail and a fine up to $10,000, if he:

- With intent to obtain a benefit fraudulently, presents or uses a credit card with knowledge that the card, whether or not expired, has not been issued to him and is not used with the effective consent of the cardholder; or the card has expired, or has been revoked or cancelled;
- With intent to obtain a benefit, uses a fictitious credit card or debit card or the pretended number or description of a fictitious card;
- Receives a benefit that he knows has been obtained in violation of this section;
- Steals credit card or debit card or, with knowledge that it has been stolen, receives a credit card or debit card with intent to use it, to sell it, or to transfer it to a person other than the issuer or the cardholder;
- Buys a credit card or debit card from a person who he knows is not the issuer;
- Not being the issuer, sells a credit card or debit card; or
- Not being the cardholder, and without the effective consent of the cardholder, possesses a credit card or debit card with intent to use it.

Statute: Penal Code: §32.31:
http://www.statutes.legis.state.tx.us/SOTWDocs/PE/htm/PE.32.htm#32.31

A person commits an offense if he intentionally or knowingly makes a materially false or misleading written statement to obtain property or credit for himself or another. An offense is a Class C misdemeanor if the value of the property or the amount of credit is less than $50; a Class B misdemeanor if the value is between $50 and $500; a Class A misdemeanor if the value is between $500 and $1500; a state jail felony if between $1500 and $20,000; a felony of the third degree if the value is between $20,000 and $100,000; a felony of the second degree if the value

is between $100,000 and $200,000; and a felony of the first degree if the value is more than $200,000.
Statute: Penal Code: §32.32:
http://www.statutes.legis.state.tx.us/SOTWDocs/PE/htm/PE.32.htm#32.32

State law authorizes businesses to require a customer to verify his identity by means of stating the zip code associated with the card, and allows the business to electronically verify with the credit card issuer that the zip code matches any zip code that the issuer has on file for the card.
Statute: Business & Commerce: §35.64:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.35.htm#35.64

Scanning Devices: State law prohibits the use of a scanning device or re-encoder that is used to obtain or record encoded information from the magnetic strip of a payment card without the authorization of the authorized user and with the intent to defraud the authorized user, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card. A re-encoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are Class B misdemeanor, punishable by 180 days in state jail and/or a fine up to $2000.
Statute: Business & Commerce: §35.60:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.35.htm#35.60

Spyware: State law prohibits the unauthorized installation or use of spyware, software that aids in gathering information about a person without his knowledge. It prohibits the unauthorized collection, transmission, and use of personally identifiable information about a person using a computer. It establishes a cause of action for providers of computer software, for the owner of a webpage or trademark and for a telecommunications carrier or Internet service provider who are adversely affected. The bill also allows the Attorney General to collect civil penalties.
Statute: Business & Commerce: §48.001 to 48.102:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.48.v2.htm

Social Security Numbers: State law restricts the public availability of Social Security numbers. It prohibits the public display or disclosure of Social Security numbers in mail, on receipts, and on the Internet. It also prohibits requiring an individual to transmit his social security number over the Internet unless the connection with the Internet is secure or the number is encrypted. The law also prohibits requiring an individual's Social Security number for access to an Internet website, unless a password or unique personal identification number or other authentication device is also required for access.
Statute: Business & Commerce: 35.58:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.35.htm#35.58

Businesses are prohibited from requiring the disclosure of a Social Security number to obtain goods or services unless the business has a privacy policy and maintains the confidentiality of that social security number. The privacy policy must include how the personal information is collected, how and when the information is used, how it is protected, who has access to it, and

how the information is disposed. A violation of the bill results in a civil fine limited to $500 for each calendar month in which one or more violations occur.
Statute: Business & Commerce: §35.581:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.35.htm#35.581

Destruction of Records: State law requires businesses to destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by shredding, erasing, or otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means.
Statute: Business & Commerce: §48.102:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.48.htm#48.102

Victim Assistance:

Mandatory Police Reports: State law requires law enforcement officers to create a written report whenever a consumer alleges being a victim of identity crime. The report must include the name of the victim, suspect (if known), type of identifying information obtained, possessed, transferred or used, and the results of the investigation. This report can be provided to the victim, upon his request.
Statute: Code of Criminal Procedure: §2.29:
http://www.statutes.legis.state.tx.us/SOTWDocs/CR/htm/CR.2.htm#2.29

Restitution: The court may order defendants convicted of identity theft offenses to make restitution to the victim, including lost income or other expenses, other than attorney's fees, incurred as a result of the offense.
Statute: Penal Code §32.51:
http://www.statutes.legis.state.tx.us/SOTWDocs/PE/htm/PE.32.htm#32.51

Security Freeze: All Texas consumers are allowed to place security freezes on their consumer credit reports to prevent new accounts from being opened in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information.

To request a freeze, a consumer must request one in writing by certified mail. The credit reporting agency may not charge a fee to victims of identity theft, who have a valid copy or a police report, investigative report, or a complaint with a governmental agency about unlawful use of his personal information by another person, for placing, temporarily lifting, or removing a security freeze on their credit report. For all other consumers, a $10 fee will be applied to place, temporarily lift or remove a security freeze on their credit report. A $12 fee may be charged for the release of a credit report to a specific person. The reporting agency must place the freeze within five business days after receiving the request, and within ten days must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time. Requests for a temporary unlocking of the freeze must be completed within three business days.

The attorney general may file suit against credit reporting agencies that violate these provisions. The suit can include injunctive relief to prevent or restrain violations, a civil penalty of up to $2,000 per violation, and if found liable, reasonable attorneys' fees, court and investigative costs, and expenses.
Statute: Business & Commerce Code: §20.034-039:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.20.htm#20.034
How To Place a Security Freeze: http://www.consumersunion.org/pdf/security/securityTX.pdf

Security Breach: State law requires a person or business that conducts business in the state and owns or licenses computerized data that includes the sensitive personal information of a state resident to notify any resident of the state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A security breach occurs upon "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information."

Sensitive personal information is defined as an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: Social Security number; driver's license number or government-issued identification number; or an 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. It does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Notice must be made as quickly as possible, but may be delayed upon the request of law enforcement or to determine the scope of the breach, or to restore the reasonable integrity of the data system. Notification can be provided by mail or e-mail. If the cost of providing regular notice would exceed $250,000, the amount of people to be notified exceeds 500,000, or the person or business does not have sufficient contact information to provide written or electronic notice, substitute notice may be provided. When substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the person's or business's web site, and notification to statewide media. If the number of affected consumers is 10,000 or more, the consumer reporting agencies must also be notified.
Statute: Business & Commerce: §48.103:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.48.htm#48.103

Court Orders: State law permits identity theft victims to file an application with the district court for the issuance of court order to declare them a victim of identity theft. To file such an application, a person must have already filed a criminal complaint with a law enforcement agency or have been injured (financially or otherwise) as a result of the identity theft crime. The court will hold a hearing where the victim will present his evidence, and if the court is satisfied, it will enter an order declaring him to be "a true victim of identity theft." This order can be used to dispute and correct business or governmental records that contain inaccurate or false information that resulted from the identity theft.
Statute: Business & Commerce Code: §48.202:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.48.htm#48.202

Security Alerts: A consumer may place a security alert on his credit reports, signifying the fact that his identity may have been used without his consent to fraudulently obtain goods or services in the his name. The alert requires potential creditors to take reasonable steps to verify the consumer's identity, including contacting the consumer at a specified phone number, before extending credit. The credit reporting agency must comply within 24 hours of receiving a consumer's request to place a security alert, and must show it to those who request your credit report for 45 days. It can be extended for additional periods upon request.
Statute: Business & Commerce Code: §20.031-033:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.20.htm#20.032

Prohibition Against Discrimination in Extending Credit: State law prohibits credit issuers from denying or restricting credit to someone simply because he or she has been a victim of identity theft, as long as the victim has filed a criminal complaint of the theft.
Statute: Business & Commerce Code: §35.585:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.35.htm#35.585

Prohibitions Against Debt Collectors: State law prohibits debt collectors from pursuing collection of a debt if: the charges were made by an unauthorized user, the debt collector received written notice that the charge was unauthorized, and the authorized user filed a police report that the charges were unauthorized and provided the debt collection agency with a copy of that report.
Statute: Finance Code: §392.303:
http://www.statutes.legis.state.tx.us/SOTWDocs/FI/htm/FI.392.htm#392.303

Criminal History Records: Once informed that a person's identifying information was falsely given by an arrested person, local law enforcement agencies are required to contact the person whose identity has been falsely used and give that person notice of his or her rights. This includes filing a declaration within the Department of Public Safety (DPS), and expunction of information. If local law enforcement is unable to do so, DPS must make the notification. In addition, DPS must make certain computerized criminal history information reflects the use of the person's identity as a stolen alias, and, when applicable, notify the Texas Department of Criminal Justice (TDCJ) that one of its inmates may be falsely using the person's identity.
Statute: Code of Criminal Procedure: §2.28:
http://www.statutes.legis.state.tx.us/SOTWDocs/CR/htm/CR.2.htm#2.28

Check Verification Service Notification: State law requires banks to offer its customers the option of having the bank notify the check verification services that the customer is a victim of identity theft. If a customer notifies the financial institution that he/she is a victim of identity theft, requests that the institution close an account that has been compromised by the alleged offense, and presents a copy of a police report and a sworn statement that he/she is a victim of identity theft, the financial institution must convey this information to the check verification entities through a secure electronic notification system. Victims also have the right to contact the check verification entities directly.
Statute: Business & Commerce Code: §35.595:
http://www.statutes.legis.state.tx.us/SOTWDocs/BC/htm/BC.35.htm#35.595

State Resources:

"Fighting Identity Theft" (www.texasfightsidtheft.gov)
This comprehensive Web site includes information on how to prevent and respond to identity crimes.

- "If You're A Victim" (http://www.texasfightsidtheft.gov/tasks.shtml)
  This directs victims to: "*Report the crime to your local law enforcement agency. Ask for a copy of the police report and case number.*" It includes tips for victims to prepare for their visit to the police department to report the crime.
- "Preventing Identity Theft" (http://www.texasfightsidtheft.gov/preventing.shtml)
- "Watching for Identity Theft" (http://www.texasfightsidtheft.gov/watching.shtml)

"Identity Theft Victim's Kit" (http://www.texasfightsidtheft.gov/pdfs/IDTheft_kit.pdf)
This comprehensive 45-page document contains detailed checklists of steps identity theft victims should take to clear their name with both creditors and law enforcement agencies. It includes several important forms, including the "ID Theft Affidavit," "Fraudulent Account Statement," and "Application for Court Order."

Victims Initiative for Counseling, Advocacy, and Restoration of the Southwest (VICARS) (http://www.idvictim.org/).
VICARS is a program of the Texas Legal Services Center that provides free civil legal services to victims of identity theft and financial fraud.

- "Victim's Toolkit" (http://www.idvictim.org/LocalResources.cfm?pagename=Victim%27s%20Toolkit)

Office of the Attorney General, "Identity Theft"
(http://www.oag.state.tx.us/consumer/identity_theft.shtml),
(Printer Friendly: http://www.oag.state.tx.us/AG_Publications/pdfs/idtheft_pf.pdf)
This document includes the recommendation that victims: "*File a police report with your local law enforcement agency and keep a copy of that report. Many banks and credit agencies require such a report before they will acknowledge that a theft has occurred.*"

"Identity Theft" Brochure (http://www.oag.state.tx.us/AG_Publications/pdfs/idtheft.pdf)

Department of Public Safety, "Identity Theft Information Guide: What to Do If You Have Become a Victim of Identity Theft"
(http://www.txdps.state.tx.us/administration/driver_licensing_control/idtheft/idtheft2.htm)
This document contains a checklist of steps an identity theft victim should take: "*An individual who believes that their identity has been fraudulently used must contact their local Sheriff's Office or City Police Department to file a report that his/her identity has been used by another person without their consent. List exactly what has happened, such as bad checks, credit card abuse, or misuse of name, state driver license, or identification card. The Sheriff's Office or Police Department can then report that information to a statewide file managed by the Department of Public Safety.*"

Legislation:

2007:
SB 222 expands the state's security freeze law to all consumers. Previously, only identity theft victims were allowed to place security freezes on their consumer credit reports to prevent new accounts from being opened in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information.

To request a freeze, a consumer must request one in writing by certified mail. The credit reporting agency may not charge a fee to victims of identity theft. For all other consumers, a $10 fee will be applied to place, temporarily lift or remove a security freeze on their credit report. A $12 fee may be charged for the release of a credit report to a specific person.

HB 2002 will require banks to offer its customers the option of having the bank notify the check verification services that the customer has been a victim of identity theft. This prevents the check verification services from continuing to cash bad checks in the customer's name, unaware that the customer is a victim of identity theft. If a customer notifies the financial institution that he/she is a victim of identity theft, requests that the institution close an account that has been compromised by the alleged offense, and presents a copy of a police report and a sworn statement that he/she is a victim of identity theft, the financial institution must convey this information to the check verification entities through a secure electronic notification system. Individuals also have the right to contact the check verification entities directly.

HB 649 expands the offense of fraudulent use or possession of identifying information to include obtaining, possessing, transferring, or using the identifying information of a child younger than 18, with the intent to hard or defraud another.

HB 460 expands the state's identity theft to include obtaining, possessing, transferring, or using, with the intent to harm or defraud another and without legal authorization, an item of identifying information of a deceased person, including a stillborn infant or fetus. The bill also restructures the punishment for the offense to enhance the punishment based on the number of items possessed. It is now a state jail felony if the number of items obtained, possessed, transferred or used is less than five; a felony of the third degree if the number is five to nine; a felony of the second degree if the number is ten to 49; and a felony of the first degree if 50 or more.

HB 887 increases the statute of limitation for identity theft crimes from three years to seven years. It also increases the statute of limitations for credit or debit card abuse and false statement to obtain property or credit to seven years.

HB 3093 seeks to decrease credit card fraud by authorizing businesses to check a customer's identity by verifying a zip code associated with that credit card with the credit card issuing company.

2005:
The legislature passed a comprehensive identity theft bill (**SB 122)**. The bill:

- Grants the Office of the Attorney General more authority to file suit against people who commit identity theft, including restitution to victims and fines from $2,000 to $50,000 per violation.
- Requires companies and public entities that discover a security breach that can lead to identity theft will be required to notify affected individuals.
- Requires law enforcement officers to create a written report whenever a consumer alleges being a victim of identity crime. The report must include the name of the victim, suspect (if known), type of identifying information obtained, possessed, transferred or used, and the results of the investigation.
- Gives victims the option to file an application with the district court for the issuance of court order to declare them a victim of identity theft.

HB 1098 targets phishing scams, in which identity thieves try to trick consumers out of personal information by sending fraudulent e-mails, purporting to originate from a familiar institution, such as a bank. The bill prohibits a person from creating a web page or domain name without the express authority of the registered owner of the business to induce, request or solicit another person to provide identifying information. Internet service providers and owners of websites or trademarks affected by the phishing scan can file suit against the phishers to seek up to $100,000 for each violation or actual damages, whichever is greater. Punitive damages are available for repeat offenders. There is no private course of action for individuals.

HB 1430 / SB 327 prohibits the unauthorized installation or use of spyware, computer software that aids in gathering information about a person without his knowledge. Spyware can be downloaded onto a person's computer when the person installs a new program and in many cases, users are unaware that they have installed spyware. The bill creates an offense and penalty for the unauthorized collection, transmission, and use of personally identifiable information about a person using a computer. It establishes a cause of action for providers of computer software, for the owner of a webpage or trademark and for a telecommunications carrier or Internet service provider who are adversely affected. The bill also allows the Attorney General to collect civil penalties.

HB 982 requires restaurant and bar owners to post signs that tell employees that tampering with someone's credit card is a felony punishable by two years in jail. The state will levy a fine of $25 on restaurateurs who do not comply until they do. It is designed to deter waiters and bartenders from copying customers' credit card numbers by swiping the card through a small gadget called a skimmer. This device records the names, account numbers and other identifying information stored in cards' magnetic strips. Later, criminals can transfer the information to a personal computer, and from there, they can sell the number, use it to finance a personal Internet shopping spree or make new cards. The Web also can be the source for blank credit cards and machines that can encode them with your number.

HB 1130 prohibits a business from requiring the disclosure of a Social Security number to obtain goods or services unless the business has a privacy policy and maintains the confidentiality of that social security number. The privacy policy must include how the personal information is

collected, how and when the information is used, how it is protected, who has access to it, and how the information is disposed. A violation of the bill results in a civil fine limited to $500 for each calendar month in which one or more violations occur.

SB 99 provides that credit issuers may not deny or restrict credit to someone simply because he or she has been a victim of identity theft, as long as the victim has filed a criminal complaint of the theft.

HB 698 requires that business records containing personal identifying information be shredded, erased, or destroyed by other means prior to disposal. Violators will be liable for a civil penalty of up to $500 for each record. The attorney general may bring an action against the business to recover the civil penalty, obtain any other remedy, including injunctive relief, and recover costs and reasonable attorney's fees.

HB 628 prohibits debt collectors from pursuing collection of a debt if: the charges were made by an unauthorized user, the debt collector received written notice that the charge was unauthorized, and the authorized user filed a police report that the charges were unauthorized and provided the debt collection agency with a copy of that report.

HB 2223 seeks to make it easier for victims of forged checks to clear their record. Under the bill, banks must mark checks as "forged" or "fraudulent" if the account owner proves that he or she has been the victim of identity theft.

SB 1485 allows governments to block out Social Security numbers in order to protect a person's privacy and keep an individual's Social Security number from inadvertently being released to the public.

2003:

HB 254 allows identity theft to be prosecuted in any county in which the offense was committed or in the home county of the victim.

SB 473 will allow consumers to issue a credit alert or even place a freeze on their credit file if they suspect that they have been victims of identity. Issuing an alert makes credit companies call the consumer first before issuing credit, while a freeze prohibits a consumer-reporting agency from releasing credit information about a consumer. A consumer-reporting agency must place a security alert on a consumer's file within 24 hours of receiving the consumer's request to do so, and the alert must remain in effect for at least 45 days. Upon a request that includes a copy of a valid police report or complaint of identity theft, an agency must place a security freeze on a consumer's file within five business days.

In addition, the bill also seeks to help reduce the risk of identity theft by restricting public availability of Social Security numbers. Effective January 1, 2005, it will prohibit the public display or disclosure of social security numbers in mail, on receipts, and on the Internet. The bill's provisions for confidentiality of social security numbers would not apply to the public sector because of the cost of converting records.

SB 566 requires a local law enforcement agency, if informed that a person's identifying information was falsely given by a person arrested as the arrested person's identifying information, to contact the person whose identity has been falsely used and give that person notice of his or her rights. Under previous law, a person whose identity has been falsely used by another person who has committed a crime had no way of knowing that his or her name was given to law enforcement at the time of the arrest.

The bill requires the Department of Public Safety (DPS) to notify the victim of the identity theft if local law enforcement is unable to do so, make certain computerized criminal history information reflects the use of the person's identity as a stolen alias, and, when applicable, notify the Texas Department of Criminal Justice (TDCJ) that one of its inmates may be falsely using the person's identity.

HB 2138 takes aim at a popular tool for identity theft by making it a crime to use an electronic credit card reader, known as a “skimmer,” to make illegal versions of customers' credit card information. It provides that it is an offense for a person to use a skimmer or re-encoder to access, read, scan, store, or transfer the information encoded on a payment card's magnetic strip without the consent of the card's authorized user.

SB 235 requires that credit or debit card receipts include no more than the last four digits of the account number. Receipts also can no longer include the card's expiration date.

HB 325 increases the penalty for refusing to provide identity information or providing false identity information to a peace officer.