

NEW MEXICO

IDENTITY THEFT RANKING BY STATE: Rank 9, 87.5 Complaints Per 100,000 Population,
1723 Complaints (2007)

Updated September 1, 2008

Current Laws: Theft of identity consists of willfully obtaining, recording, or transferring personal identifying information of another person without the authorization or consent of that person and with the intent to defraud that person or another.

“Personal identifying information” is defined as information that alone or in conjunction with other information identifies a person, including the person’s name, address, telephone number, driver’s license number, Social Security number, place of employment, maiden name of the person’s mother, demand deposit account number, checking or savings account number, credit card or debit card number, personal identification number, passwords or any other numbers or information that can be used to access a person’s financial resources.

Theft of identity is a fourth class felony, punishable by eighteen months in jail and/or a fine up to \$5,000.

Statute: §30-16-24.1: www.nmlaws.org (must click on “Statutes” and then “Statutory Chapter” in the left-hand menu, and then select the appropriate chapter and statute.)

Phishing: State law prohibits phishing, a form of identity theft when someone sends an e-mail that looks official but is used to trick the recipient into giving away personal information that can be used to access a person's financial accounts or obtain goods and services. The law covers obtaining identity by electronic fraud, which consists of knowingly and willfully soliciting, requesting, or taking any action by means of a fraudulent electronic communication with intent to obtain the personal identifying information of another. It prohibits a person from sending e-mails that falsely represent another legitimate business and prohibits linking or sending the e-mail recipient to a false Web page in order to collect identifying information. It is also unlawful to obtain identifying information from the e-mail recipient, directly or indirectly, for activities the recipient thinks is valid. Obtaining identity by electronic fraud is a fourth class felony, punishable by eighteen months in jail and/or a fine up to \$5,000.

Statute: §30-16-24.1: www.nmlaws.org (must click on “Statutes” and then “Statutory Chapter” in the left-hand menu, and then select the appropriate chapter and statute.)

Jurisdiction: Theft of identity and obtaining identity by electronic fraud are considered to have been committed in the county where the person whose identifying information was appropriated, obtained or sought resided at the time of the offense; or the county in which any part of the offense took place, regardless of whether the defendant was ever actually present in the county.

Statute: §30-16-24.1: www.nmlaws.org (must click on “Statutes” and then “Statutory Chapter” in the left-hand menu, and then select the appropriate chapter and statute.)

Payment Cards: Fraudulent use of a credit card consists of a person obtaining anything of value, with intent to defraud, by using a credit card obtained fraudulently or an invalid, expired, or revoked credit card; by fraudulently representing himself as the cardholder, or by having a credit card issued in the name of another person without the consent of the original cardholder. Punishment depends on the value of the property or service obtained with the card. It ranges from a petty misdemeanor if the value is less than \$250 in a six-month period; a misdemeanor if between \$250 and \$500, a fourth degree felony if between \$500 and \$2500, a third degree felony if between \$2500, and \$20,000, and a second-degree felony if above \$20,000. Statute: §30-16-33: www.nmlaws.org (must click on “Statutes” and then “Statutory Chapter” in the left-hand menu, and then select the appropriate chapter and statute.)

Anyone, other than the issuers, who possesses, receives, sells or transfers four or more credit cards, issued in a name or names other than his own is guilty of a third degree felony, punishable by three years in jail and/or a fine of up to \$5000.

Statute: §30-16-30: www.nmlaws.org (must click on “Statutes” and then “Statutory Chapter” in the left-hand menu, and then select the appropriate chapter and statute.)

Social Security Numbers: State law restricts the public disclosure of Social Security numbers (SSNs) in order to prevent identity theft. It prohibits businesses from making the complete number available to the general public, including intentionally communicating a SSN to the general public or printing a SSN on a receipt issued for the purchase of products or services, including receipts for purchases of services from the state or its political subdivisions. It prevents businesses from printing a SSN on any card or material mailed to an individual unless required by federal law. It also prohibits companies from requiring a consumer to transmit a SSN over the Internet, unless the connection is secure or the SSN is encrypted, and from requiring an individual to use his/her SSN to access the Web site, unless a password or unique personal identification number or other authentication device is also required to access the site. Statute: § 57-12B-1 through 4: www.nmlaws.org (must click on “Statutes” and then “Statutory Chapter” in the left-hand menu, and then select the appropriate chapter and statute.)

Victim Assistance:

Restitution: In addition to any other punishment, a person found guilty of theft by identity or of obtaining identity by electronic fraud will be ordered to make restitution for any financial loss sustained by a person injured as the direct result of the offense. In addition to out-of-pocket costs, restitution may include payment for costs, including attorney fees, incurred by the victim in clearing his/her credit history or credit rating, or costs incurred in connection with a civil or administrative proceeding to satisfy a debt, lien, judgment, or other obligation.

Statute: §30-16-24.1: www.nmlaws.org (must click on “Statutes” and then “Statutory Chapter” in the left-hand menu, and then select the appropriate chapter and statute.)

Security Freeze: All consumers are permitted to place a security freeze on their credit reports. A security freeze prohibits, with certain specific exceptions, the credit reporting agency from releasing the consumer’s credit report or any information from it without the express authorization of the consumer. This prevents a credit file from being shared with potential creditors, blocking new accounts from being opened. To obtain a security freeze, consumers

must send a credit reporting agency a written request by certified mail, provide proper identification and pay a fee, if applicable. The credit reporting agencies are permitted to charge a fee of \$10 for the placement of a security freeze, \$5 for the release of a credit report to a specific person or for a specific period of time, and \$5 to remove the freeze. However, there is no charge for victims of identity theft who provide a copy of a police report and for people 65 years of age or older.

Credit reporting agencies must place the freeze within three business days of receiving the request, and within five days, must provide the consumer with written confirmation of the freeze and a unique personal identification number, password or similar device to be used by the consumer when providing authorization for the release of the consumer's credit report to a specific person or for a specific period of time or for permanent removal of the freeze. Requests for a temporary unlocking of the freeze must be completed within three business days. However, temporary unlocking must be completed within 15 minutes after the consumer's request is received through an electronic contact method or by telephone, during normal business hours. Statute: §56-3A1 through 6: www.nmlaws.org (must click on "Statutes" and then "Statutory Chapter" in the left-hand menu, and then select the appropriate chapter and statute.)

State Resources:

"Identity Theft Repair Kit" (<http://nmag.gov/pdf/ID%20Theft%20broch.pdf>)

This comprehensive guide for victims includes helpful checklists for actions to take, based on the identifying documents that were stolen. It directs victims to first: *"Contact the Police: File a report with your local police department and, if the identity theft did not take place within your area, file a report with the police from the area where the theft took place. Make sure to get a copy of the police report. You may need that documentation to support your claims to credit bureaus, creditors, debt collectors, or other companies. If you are unable to obtain a copy of the police report, be sure to get the report number."*

"Protecting Your Identity Online"

(<http://www.nmag.gov/office/Divisions/Com/InternetSafety/identity.aspx>)

This document directs victims of identity theft to: *"Immediately file a police report and retain a copy."*

Securities Division, "Foiling Identity Theft"

(<http://www.rld.state.nm.us/Securities/PDFs/IDtheftBrochure.pdf>)

Aging and Long Term Services Department, "Senior Safety: Identity Theft"

(<http://www.nmaging.state.nm.us/idtheft.html>)

Legislation:

2007:

SB 165 allows all consumers in the state to place a security freeze on their credit reports to prevent an identity thief from opening an account or obtaining credit under their name. The security freeze can be lifted for a specific time to open an account or make a major purchase. Credit reporting agencies will have a maximum of three days to put the security freeze in place after a request. To obtain a security freeze, consumers must send a credit reporting agency a written request by certified mail, provide proper identification and pay a fee, if applicable. The agencies can charge \$10 to place a freeze, and \$5 to temporarily or permanently lift the freeze, but identity theft victims with a police report and people 65 or older will not have to pay for the freeze.

2005:

SB 720 makes identity theft a fourth-degree felony, punishable by up to 18 months in prison. Previously it was a misdemeanor. The bill also specifically outlaws the use of computers and electronic equipment to defraud or otherwise steal an individual's personal or financial identifying information, which is then used to strip their assets or destroy their credit rating. Commonly known as "phishing," the crime of obtaining identity by electronic fraud is defined as using email, a web site or other electronic communication to obtain the personal identifying information of another person by false pretenses.

HB 363 restricts the public disclosure of Social Security numbers (SSNs) in order to prevent identity theft. It prohibits businesses from making the complete number available to the general public, including intentionally communicating a SSN to the general public or printing a SSN on a receipt issued for the purchase of products or services, including receipts for purchases of services from the state or its political subdivisions. It prevents businesses from printing a SSN on any card or material mailed to an individual unless required by federal law. It also prohibits companies from requiring a consumer to transmit a SSN over the Internet, unless the connection is secure or the SSN is encrypted, and from requiring an individual to use his/her SSN to access the Web site, unless a password or unique personal identification number or other authentication device is also required to access the site.

2001:

HB 317 creates a new crime of theft of identity for people who take personal identification information, such as a Social Security number or account passwords, without the owner's consent, and use it to obtain money, credit or anything of value.