

NEBRASKA

IDENTITY THEFT RANKING BY STATE: Rank 40, 44.7 Complaints Per 100,000
Population, 793 Complaints (2007)
Updated December 21, 2008

Current Laws:

Identity Crime: A person commits the crime of criminal impersonation if he or she:

- Assumes a false identity with intent to gain a pecuniary benefit for himself, herself, or another or to deceive or harm another person;
- Without the authorization or permission of another and with the intent to deceive or harm another, obtains or records personal identification documents or personal identifying information, and accesses or attempts to access the financial resources of another through the use of a personal identification document or personal identifying information for the purpose of obtaining credit, money, goods, services, or any other thing of value.

Violations are punished based on the value of credit, money, goods, services, or other thing of value that was gained or attempted to be gained:

Value of credit, money, goods, services, or other thing of value that was gained or was attempted to be gained	Offense Level	Maximum Penalty –Term of Imprisonment/Fine
Less than \$200	Class II misdemeanor	6 months / \$1,000
Second conviction	Class I misdemeanor	1 year / \$1,000
Third or subsequent conviction	Class IV felony	5 years / \$10,000
\$200-\$499	Class I misdemeanor	1 year / \$1,000
Second or subsequent conviction	Class IV felony	5 years / \$10,000
\$500-\$1,499	Class IV felony	5 years / \$10,000
\$1,500 or more	Class III felony	20 years / \$25,000 (minimum 1 year)

“Personal identification document” includes a birth certificate, motor vehicle operator’s license, state ID card, employment ID card, Social Security card, or passport, or any document made or altered in a manner that it purports to have been made on behalf of or issued to another person by the authority of a person who did not give that authority.

“Personal identifying information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including a person’s name; date of birth; address; motor vehicle operator’s license number or state ID card number; Social Security number or work permit number; employment ID card; maiden name of a person’s mother; credit or debit card number; bank account number; electronic ID number, address, or routing code used to access financial information; digital signature; telecommunications identifying information or access device; unique biometric data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation; and any other number or information which can be used to access a person’s financial resources.

Statute: §28-608: <http://law.justia.com/nebraska/codes/s28index/s2806008000.html>

Payment Cards: A person commits the offense of unauthorized use of a financial transaction device (such as a credit card or debit card) if he uses the device in an automated banking device, to imprint a sales form, or in any manner for the purpose of obtaining money, credit, property, or services or for making financial payment, with intent to defraud, while knowing that the device is expired or revoked or forged, altered or counterfeited, or when for any reason his use of the device is unauthorized either by the issuer or the account holder. It is a class II misdemeanor if the total value of the money, credit, property, or services obtained is less than \$200 in a six-month period from the date of the first unauthorized use. It is a class I misdemeanor if the value is \$200-\$500 in a six-month period; a class IV felony if the value is \$500 to \$1500 in a six-month period; and a class III felony if it is over \$1500. Prosecutions may be conducted in any county where the person committed the offense.

Statute: §28-620: <http://law.justia.com/nebraska/codes/s28index/s2806020000.html>

A person commits the crime of criminal possession of a financial transaction device if, with the intent to defraud, a person possesses any financial transaction card issued to a different account holder or which he knows or reasonably should know to be lost, stolen, forged, altered, or counterfeited. It is a class III misdemeanor if the person possesses one such device; a class IV felony if he possesses two or three such devices, each issued to different account holders; and a class III felony if he possess four or more devices, each issued to different account holders.

Statute: §28-621: <http://law.justia.com/nebraska/codes/s28index/s2806021000.html>

A person commits the crime of unlawful circulation of a financial transaction device in the first degree if he sells or possesses with the intent to sell two or more such devices that he knows or reasonably should know to be lost, stolen, forged, altered, counterfeited, or delivered under mistake. This is a class III felony.

Statute: §28-622: <http://law.justia.com/nebraska/codes/s28index/s2806022000.html>

If a person sells or possesses with the intent to sell one financial device, it is unlawful circulation of a financial transaction device in the second degree, a class IV felony.

Statute: §28-623: <http://law.justia.com/nebraska/codes/s28index/s2806023000.html>

Scanning Devices: State law prohibits the use of a scanning device or re-encoder to obtain or record encoded information from the magnetic strip of a payment card 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 a class IV felony. Second or subsequent offenses are a class IIIA felony. Statute: §28-634: <http://law.justia.com/nebraska/codes/s28index/s2806034000.html>

Social Security Numbers: An employer may not:

- Publicly post or publicly display in any manner more than the last four digits of an employee's Social Security number (SSN), including intentional communication of more than the last four digits or otherwise making more than the last four digits available to the general public or an employer's coworkers;
- Require an employee to transmit more than the last four digits of his or her SSN over the Internet unless the connection is secure or the information is encrypted;
- Require an employee to use more than the last four digits of his or her SSN to access an Internet web site unless a password, unique personal identification number, or other authentication device is also required to access the site;
- Require an employee to use more than the last four digits of his or her SSN as an employee number for any type of employee-related activity.
- Use a SSN as an identification number of occupational licensing or as an identification number for company meetings.

An employer may use more than the last four digits of an employee's SSN only for compliance with state or federal laws, rules, or regulations; internal administrative purposes, including provision of SSNs to third parties for administration of personnel benefit provisions for the employer and employment screening and staffing; and commercial transactions between the employer and employee. Employees' SSNs may not be kept in files with unrestricted access within the company. Violations are a Class V misdemeanor.

Statute: §48-237: <http://www.nebraskalegislature.gov/laws/statutes.php?statute=s4802037000>

Victim Assistance:

Restitution: In addition to criminal penalties and fines, a person convicted of criminal impersonation may be ordered to make restitution to the victim based on the actual damages sustained by the victim.

Statute: §28-608: <http://law.justia.com/nebraska/codes/s28index/s2806008000.html>

Security Freeze: All Nebraska consumers are allowed to place security freezes on their consumer credit reports to prevent others from opening new accounts 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 or overnight mail to the credit reporting agencies. The agency may charge a one-time fee of \$15 for placing a security freeze. However, it may not charge a fee to minors or to identity theft victims who provide a copy of an official police report documenting the identity theft. There is no fee for any consumer for the release of a credit report for a specified period of time or for removal of the freeze.

The reporting agency must place the freeze within three business days after receiving the request. Within five business days, it 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. Starting January 1, 2009, consumer reporting agencies must have in place procedures involving the use of a telephone, the Internet, or other electronic media to receive and process a request for a temporary lift of a security freeze. If a request is received in this manner during normal business hours, the freeze must be lifted within fifteen minutes.

Statute: §8-2601 to 8-2615: <http://www.nebraskalegislature.gov/laws/browse-chapters.php?chapter=08> (must scroll down to relevant sections)

How to Place a Security Freeze in Nebraska:

<http://www.consumersunion.org/pdf/security/securityNE.pdf>

State Resources:

Office of the Attorney General, “Identity Theft”

(<http://www.ago.ne.gov/consumer/idtheftinfo.htm>)

“Identity Theft Repair Kit” (http://www.ago.state.ne.us/media/AGO_IDTheftBroch.pdf)

This comprehensive document contains an extensive checklist of steps that identity theft victim should take, including filing a report with local law enforcement: *“Step 1: 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. 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.”*

Cybersecurity Center, “Identity Theft” (<http://its.ne.gov/cybersecurity/idtheft/>)

This document includes prevention tips and instructions for victims. It directs victims to: *“File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.”*

Department of Motor Vehicles, “Identity Theft”

(<http://www.dmv.state.ne.us/www.dmv.state.ne.us/dvr/fraud/fraud.html>)

This page contains information on how the DMV assists victims of identity theft. It contains a link to its “ID Theft Packet” (<http://www.dmv.state.ne.us/dvr/pdf/theftpacket.pdf>), which is what the agency gives to victims who have reported suspected fraudulent activity involving their driver’s license, or vehicle registration and title documents. The forms contained in the packet must be completed and returned to the DMV before the investigative process can begin.

Legislation:

2007:

LB 674 allows all consumers to place security freezes on their consumer credit reports to prevent identity thieves from opening new accounts 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. Consumer reporting agencies may charge a one-time \$15 fee to place a security freeze, but may not charge minors or identity theft victims with a valid police report.

The bill also limits employers' use of employees' Social Security numbers (SSNs). Under the bill, employers could not post employees' Social Security numbers; allow the public or coworkers to access those numbers; require workers to use Social Security numbers to access Internet sites or send the numbers via e-mail unless the transmissions are encrypted.

2002:

LB 276 establishes the crime of identity theft, making it illegal to obtain personal identification documents and information or to access another person's financial resources using personal information without the individual's authorization or with the intent of deceiving or harming the individual. Under the new law, identity fraud involving \$500 or more will be prosecuted as a felony. If more than \$1500 is involved, perpetrators would face up to 20 years in prison. Crimes involving less than \$500 will remain misdemeanors. In addition, the law allows victims to seek restitution, attorney's fees and other costs resulting from identity fraud. The bill also requires retailers to have systems that display only the last five digits of a person's credit card number on a purchase receipt by 2007. "Skimming," the act of unlawfully obtaining information from the magnetic strip on a person's credit card, becomes a criminal act.