

HB 1832 -- MERCHANDISING PRACTICES (Cornejo)

COMMITTEE OF ORIGIN: Standing Committee on Judiciary

SCRAP METAL PURCHASES

Currently, scrap dealers must keep documentation for any transaction involving certain metals. This bill expands the documentation requirements to add transactions involving motor vehicle, heavy equipment, or tractor batteries (Section 407.300, RSMo).

CREDIT USER PROTECTION LAW

The bill states that a person commits the offense of illegal use of a card scanner if the person:

- (1) Uses a scanning device to obtain information stored on a credit card without the permission of the cardholder, credit card issuer, or merchant;
- (2) Possesses a scanning device with the intent to defraud or with the knowledge that some other person intends to use the device to defraud;
- (3) Uses a reencoder to copy a credit card without the permission of the cardholder and with the intent to defraud; or
- (4) Possesses a reencoder with the intent to defraud or with the knowledge that another person intends to use the reencoder to defraud.

The offense of illegal use of a card scanner is a class D felony for the first offense and any subsequent offense arising from a separate incident is a class C felony.

A person commits the offense of defacing a credit card reader if the person damages, defaces, alters, or destroys a scanning device and the person has no right to do so. The offense of defacing a credit card reader is a class A misdemeanor.

A violation of either of these offenses constitutes an illegal practice under current merchandising practices statutes, and a violator is subject to any penalties under these statutes. The Attorney General shall have the same powers, rights, and duties regarding violations of either of these offenses as he or she does under current merchandising practices statutes (Sections 407.431, 407.432, 407.433, and 407.436).

SAFEKEEPING OF PERSONAL INFORMATION

This bill changes the amount of time within which a person that owns or licenses personal information of residents of Missouri is required to inform an affected consumer that there has been a breach of security following discovery or notification of the breach from without unreasonable delay to within 30 days of the discovery or notification.