

SECOND REGULAR SESSION

[PERFECTED]

HOUSE BILL NO. 1832

99TH GENERAL ASSEMBLY

INTRODUCED BY REPRESENTATIVE CORNEJO.

5497H.01P

D. ADAM CRUMBLISS, Chief Clerk

AN ACT

To repeal sections 407.300, 407.432, 407.433, 407.436, and 407.1500, RSMo, and to enact in lieu thereof seven new sections relating to merchandising practices, with penalty provisions.

Be it enacted by the General Assembly of the state of Missouri, as follows:

Section A. Sections 407.300, 407.432, 407.433, 407.436, and 407.1500, RSMo, are
2 repealed and seven new sections enacted in lieu thereof, to be known as sections 407.300,
3 407.431, 407.432, 407.433, 407.435, 407.436, and 407.1500, to read as follows:

407.300. 1. Every purchaser or collector of, or dealer in, junk, scrap metal, or any
2 secondhand property shall keep a register containing a written or electronic record for each
3 purchase or trade in which each type of ~~metal~~ **material** subject to the provisions of this section
4 is obtained for value. There shall be a separate record for each transaction involving any:

5 (1) Copper, brass, or bronze;

6 (2) Aluminum wire, cable, pipe, tubing, bar, ingot, rod, fitting, or fastener;

7 (3) Material containing copper or aluminum that is knowingly used for farming purposes
8 as farming is defined in section 350.010; whatever may be the condition or length of such metal;
9 ~~or~~

10 (4) Catalytic converter; **or**

11 (5) **Motor vehicle, heavy equipment, or tractor battery.**

12 2. The record required by this section shall contain the following data:

EXPLANATION — Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted from the law. Matter in **bold-face** type in the above bill is proposed language.

13 (1) A copy of the driver's license or photo identification issued by the state or by the
14 United States government or agency thereof to the person from whom the material is obtained;

15 (2) The current address, gender, birth date, and a photograph of the person from whom
16 the material is obtained if not included or are different from the identification required in
17 subdivision (1) of this subsection;

18 (3) The date, time, and place of the transaction;

19 (4) The license plate number of the vehicle used by the seller during the transaction;

20 (5) A full description of the ~~[metal]~~ **material**, including the weight and purchase price.

21 3. The records required under this section shall be maintained for a minimum of twenty-
22 four months from when such material is obtained and shall be available for inspection by any law
23 enforcement officer.

24 4. Anyone convicted of violating this section shall be guilty of a class B misdemeanor.

25 5. This section shall not apply to any of the following transactions:

26 (1) Any transaction for which the total amount paid for all regulated ~~[scrap metal]~~
27 **material** purchased or sold does not exceed fifty dollars, unless the ~~[scrap metal]~~ **material** is a
28 catalytic converter;

29 (2) Any transaction for which the seller, including a farm or farmer, has an existing
30 business relationship with the scrap metal dealer and is known to the scrap metal dealer making
31 the purchase to be an established business or political subdivision that operates a business with
32 a fixed location that can be reasonably expected to generate regulated scrap metal and can be
33 reasonably identified as such a business; or

34 (3) Any transaction for which the type of metal subject to subsection 1 of this section is
35 a minor part of a larger item, except for equipment used in the generation and transmission of
36 electrical power or telecommunications.

**407.431. The violation of any provision of sections 407.430 to 407.436 of this credit
2 user protection law constitutes an unlawful practice under sections 407.010 to 407.130, and
3 the violator shall be subject to all penalties, remedies, and procedures under sections
4 407.010 to 407.130. The attorney general shall have all powers, rights, and duties
5 regarding violations of sections 407.430 to 407.436 as are provided in sections 407.010 to
6 407.130, in addition to rulemaking authority under section 407.145.**

407.432. As used in sections 407.430 to 407.436, the following terms shall mean:

2 (1) "Acquirer", a business organization, financial institution, or an agent of a business
3 organization or financial institution that authorizes a merchant to accept payment by credit card
4 for merchandise;

5 (2) "Cardholder", the person's name on the face of a credit card to whom or for whose
6 benefit the credit card is issued by an issuer^[,] or any agent, authorized signatory, or employee
7 of such person;

8 (3) **"Chip", an integrated circuit imbedded in a card that stores data so that the**
9 **card may use the EMV payment method for transactions;**

10 (4) **"Contactless payment", any payment method that uses a contactless smart card,**
11 **a near field communication (NFC) antenna, radio-frequency identification (RFID)**
12 **technology, or other method to remotely communicate data to a scanning device for**
13 **transactions;**

14 (5) "Counterfeit credit card", any credit card which is fictitious, altered, or forged, any
15 false representation, depiction, facsimile or component of a credit card, or any credit card which
16 is stolen, obtained as part of a scheme to defraud, or otherwise unlawfully obtained, and which
17 may or may not be embossed with account information or a company logo;

18 ~~[(4)]~~ (6) "Credit card" ~~[or "debit card"]~~, any instrument or device, whether known as a
19 credit card, credit plate, bank service card, banking card, check guarantee card, or debit card or
20 by any other name, **that is** issued with or without a fee by an issuer for the use of the cardholder
21 in obtaining money or merchandise on credit^[,] **or by transferring payment from the**
22 **cardholder's checking account** or for use in an automated banking device to obtain any of the
23 services offered through the device. The presentation of a credit card account number is deemed
24 to be the presentation of a credit card. **"Credit card" shall include credit or debit cards**
25 **whose information is stored in a digital wallet for use in in-app purchases or contactless**
26 **payments;**

27 ~~[(5)]~~ (7) "Expired credit card", a credit card for which the expiration date shown on it
28 has passed;

29 ~~[(6)]~~ (8) "Issuer", the business organization ~~[or]~~ , financial institution, or ~~[its]~~ duly
30 authorized agent~~[, which]~~ **thereof that** issues a credit card;

31 ~~[(7)]~~ (9) "Merchandise", any objects, wares, goods, commodities, intangibles, real estate,
32 services, or anything else of value;

33 ~~[(8)]~~ (10) "Merchant", an owner or operator of any retail mercantile establishment, or
34 any agent, employee, lessee, consignee, officer, director, franchisee, or independent contractor
35 of such owner or operator. A merchant includes a person who receives from ~~[an authorized user~~
36 ~~of a payment card]~~ **a cardholder**, or an individual the person believes to be ~~[an authorized user]~~
37 **a cardholder**, a ~~[payment]~~ **credit** card or information from a ~~[payment]~~ **credit** card as the
38 instrument for obtaining, purchasing, or receiving goods, services, money, or anything of value
39 from the person;

40 ~~[(9)]~~ (11) "Person", any natural person or his legal representative, partnership, firm,
41 for-profit or not-for-profit corporation, whether domestic or foreign, company, foundation, trust,
42 business entity or association, and any agent, employee, salesman, partner, officer, director,
43 member, stockholder, associate, trustee or cestui que trust thereof;

44 ~~[(10)]~~ (12) "Reencoder", an electronic device that places encoded information from the
45 **chip or** magnetic strip or stripe of a credit ~~[or debit]~~ card onto the **chip or** magnetic strip or
46 stripe of a different credit ~~[or debit]~~ card;

47 ~~[(11)]~~ (13) "Revoked credit card", a credit card for which permission to use it has been
48 suspended or terminated by the issuer;

49 ~~[(12)]~~ (14) "Scanning device", a scanner, reader, or any other electronic device that is
50 used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information
51 **stored in the chip or** encoded on the magnetic strip or stripe of a credit ~~[or debit]~~ card.

52 **"Scanning device" shall include devices used by a merchant for contactless payments.**

407.433. 1. No person, other than the cardholder, shall:

2 (1) Disclose more than the last five digits of a credit card ~~[or debit card]~~ account number
3 on any sales receipt provided to the cardholder for merchandise sold in this state[;]

4 ~~—— (2) Use a scanning device to access, read, obtain, memorize, or store, temporarily or~~
5 ~~permanently, information encoded on the magnetic strip or stripe of a credit or debit card without~~
6 ~~the permission of the cardholder and with the intent to defraud any person, the issuer, or a~~
7 ~~merchant; or~~

8 ~~—— (3) Use a reencoder to place information encoded on the magnetic strip or stripe of a~~
9 ~~credit or debit card onto the magnetic strip or stripe of a different card without the permission~~
10 ~~of the cardholder from which the information is being reencoded and with the intent to defraud~~
11 ~~any person, the issuer, or a merchant].~~

12 2. Any person who knowingly violates this section is guilty of an infraction and any
13 second or subsequent violation of this section is a class A misdemeanor.

14 3. It shall not be a violation of subdivision (1) of subsection 1 of this section if:

15 (1) The sole means of recording the credit card number ~~[or debit card number]~~ is by
16 handwriting or, prior to January 1, 2005, by an imprint of the credit card ~~[or debit card]~~; and

17 (2) For handwritten or imprinted copies of credit card ~~[or debit card]~~ receipts, only the
18 merchant's copy of the receipt lists more than the last five digits of the account number.

19 4. This section shall become effective on January 1, 2003, and applies to any cash
20 register or other machine or device that prints or imprints receipts of credit card ~~[or debit card]~~
21 transactions and which is placed into service on or after January 1, 2003. Any cash register or
22 other machine or device that prints or imprints receipts on credit card ~~[or debit card]~~ transactions

23 and which is placed in service prior to January 1, 2003, shall be subject to the provisions of this
24 section on or after January 1, 2005.

**407.435. 1. A person commits the offense of illegal use of a card scanner if the
2 person:**

3 **(1) Directly or indirectly uses a scanning device to access, read, obtain, memorize,**
4 **or store, temporarily or permanently, information stored in the chip or encoded on the**
5 **magnetic strip or stripe of a credit card without the permission of the cardholder, the**
6 **credit card issuer, or a merchant;**

7 **(2) Possesses a scanning device with the intent to defraud a cardholder, credit card**
8 **issuer, or merchant or possesses a scanning device with the knowledge that some other**
9 **person intends to use the scanning device to defraud a cardholder, credit card issuer, or**
10 **merchant;**

11 **(3) Directly or indirectly uses a reencoder to copy a credit card without the**
12 **permission of the cardholder of the card from which the information is being reencoded**
13 **and does so with the intent to defraud the cardholder, the credit card issuer, or a**
14 **merchant; or**

15 **(4) Possesses a reencoder with the intent to defraud a cardholder, credit card issuer,**
16 **or merchant or possesses a reencoder with the knowledge that some other person intends**
17 **to use the reencoder to defraud a cardholder, credit card issuer, or merchant.**

18 **2. The offense of illegal use of a card scanner is a class D felony. However, a second**
19 **or subsequent offense arising from a separate incident is a class C felony.**

~~20 407.436. [1. Any person who willfully and knowingly, and with the intent to defraud,~~
2 ~~engages in any practice declared to be an unlawful practice in sections 407.430 to 407.436 of this~~
3 ~~credit user protection law shall be guilty of a class E felony.~~

4 ~~2. The violation of any provision of sections 407.430 to 407.436 of this credit user~~
5 ~~protection law constitutes an unlawful practice pursuant to sections 407.010 to 407.130, and the~~
6 ~~violation shall be subject to all penalties, remedies and procedures provided in sections 407.010~~
7 ~~to 407.130. The attorney general shall have all powers, rights, and duties regarding violations~~
8 ~~of sections 407.430 to 407.436 as are provided in sections 407.010 to 407.130, in addition to~~
9 ~~rulemaking authority as provided in section 407.145.]~~ **A person commits the offense of**
10 **defacing a credit card reader if a person damages, defaces, alters, or destroys a scanning**
11 **device and the person has no right to do so. The offense of defacing a credit card reader**
12 **is a class A misdemeanor.**

407.1500. 1. As used in this section, the following terms mean:

2 (1) "Breach of security" or "breach", unauthorized access to and unauthorized acquisition
3 of personal information maintained in computerized form by a person that compromises the

4 security, confidentiality, or integrity of the personal information. Good faith acquisition of
5 personal information by a person or that person's employee or agent for a legitimate purpose of
6 that person is not a breach of security, provided that the personal information is not used in
7 violation of applicable law or in a manner that harms or poses an actual threat to the security,
8 confidentiality, or integrity of the personal information;

9 (2) "Consumer", an individual who is a resident of this state;

10 (3) "Consumer reporting agency", the same as defined by the federal Fair Credit
11 Reporting Act, 15 U.S.C. Section 1681a;

12 (4) "Encryption", the use of an algorithmic process to transform data into a form in
13 which the data is rendered unreadable or unusable without the use of a confidential process or
14 key;

15 (5) "Health insurance information", an individual's health insurance policy number or
16 subscriber identification number, any unique identifier used by a health insurer to identify the
17 individual;

18 (6) "Medical information", any information regarding an individual's medical history,
19 mental or physical condition, or medical treatment or diagnosis by a health care professional;

20 (7) "Owns or licenses" includes, but is not limited to, personal information that a
21 business retains as part of the internal customer account of the business or for the purpose of
22 using the information in transactions with the person to whom the information relates;

23 (8) "Person", any individual, corporation, business trust, estate, trust, partnership, limited
24 liability company, association, joint venture, government, governmental subdivision,
25 governmental agency, governmental instrumentality, public corporation, or any other legal or
26 commercial entity;

27 (9) "Personal information", an individual's first name or first initial and last name in
28 combination with any one or more of the following data elements that relate to the individual if
29 any of the data elements are not encrypted, redacted, or otherwise altered by any method or
30 technology in such a manner that the name or data elements are unreadable or unusable:

31 (a) Social Security number;

32 (b) Driver's license number or other unique identification number created or collected
33 by a government body;

34 (c) Financial account number, credit card number, or debit card number in combination
35 with any required security code, access code, or password that would permit access to an
36 individual's financial account;

37 (d) Unique electronic identifier or routing code, in combination with any required
38 security code, access code, or password that would permit access to an individual's financial
39 account;

- 40 (e) Medical information; or
41 (f) Health insurance information.

42

43 "Personal information" does not include information that is lawfully obtained from publicly
44 available sources, or from federal, state, or local government records lawfully made available to
45 the general public;

46 (10) "Redacted", altered or truncated such that no more than five digits of a Social
47 Security number or the last four digits of a driver's license number, state identification card
48 number, or account number is accessible as part of the personal information.

49 2. (1) Any person that owns or licenses personal information of residents of Missouri
50 or any person that conducts business in Missouri that owns or licenses personal information in
51 any form of a resident of Missouri shall provide notice to the affected consumer that there has
52 been a breach of security following discovery or notification of the breach. The disclosure
53 notification shall be:

54 (a) Made ~~[without unreasonable delay]~~ **within thirty days of the discovery or**
55 **notification of the breach;**

56 (b) Consistent with the legitimate needs of law enforcement, as provided in this section;
57 and

58 (c) Consistent with any measures necessary to determine sufficient contact information
59 and to determine the scope of the breach and restore the reasonable integrity, security, and
60 confidentiality of the data system.

61 (2) Any person that maintains or possesses records or data containing personal
62 information of residents of Missouri that the person does not own or license, or any person that
63 conducts business in Missouri that maintains or possesses records or data containing personal
64 information of a resident of Missouri that the person does not own or license, shall notify the
65 owner or licensee of the information of any breach of security immediately following discovery
66 of the breach, consistent with the legitimate needs of law enforcement as provided in this section.

67 (3) The notice required by this section may be delayed if a law enforcement agency
68 informs the person that notification may impede a criminal investigation or jeopardize national
69 or homeland security, provided that such request by law enforcement is made in writing or the
70 person documents such request contemporaneously in writing, including the name of the law
71 enforcement officer making the request and the officer's law enforcement agency engaged in the
72 investigation. The notice required by this section shall be provided ~~[without unreasonable delay]~~
73 **within thirty days** after the law enforcement agency communicates to the person its
74 determination that notice will no longer impede the investigation or jeopardize national or
75 homeland security.

76 (4) The notice shall at minimum include a description of the following:

77 (a) The incident in general terms;

78 (b) The type of personal information that was obtained as a result of the breach of
79 security;

80 (c) A telephone number that the affected consumer may call for further information and
81 assistance, if one exists;

82 (d) Contact information for consumer reporting agencies;

83 (e) Advice that directs the affected consumer to remain vigilant by reviewing account
84 statements and monitoring free credit reports.

85 (5) Notwithstanding subdivisions (1) and (2) of this subsection, notification is not
86 required if, after an appropriate investigation by the person or after consultation with the relevant
87 federal, state, or local agencies responsible for law enforcement, the person determines that a risk
88 of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the
89 breach. Such a determination shall be documented in writing and the documentation shall be
90 maintained for five years.

91 (6) For purposes of this section, notice to affected consumers shall be provided by one
92 of the following methods:

93 (a) Written notice;

94 (b) Electronic notice for those consumers for whom the person has a valid email address
95 and who have agreed to receive communications electronically, if the notice provided is
96 consistent with the provisions of 15 U.S.C. Section 7001 regarding electronic records and
97 signatures for notices legally required to be in writing;

98 (c) Telephonic notice, if such contact is made directly with the affected consumers; or

99 (d) Substitute notice, if:

100 a. The person demonstrates that the cost of providing notice would exceed one hundred
101 thousand dollars; or

102 b. The class of affected consumers to be notified exceeds one hundred fifty thousand;
103 or

104 c. The person does not have sufficient contact information or consent to satisfy
105 paragraphs (a), (b), or (c) of this subdivision, for only those affected consumers without
106 sufficient contact information or consent; or

107 d. The person is unable to identify particular affected consumers, for only those
108 unidentifiable consumers.

109 (7) Substitute notice under paragraph (d) of subdivision (6) of this subsection shall
110 consist of all the following:

111 (a) Email notice when the person has an electronic mail address for the affected
112 consumer;

113 (b) Conspicuous posting of the notice or a link to the notice on the internet website of
114 the person if the person maintains an internet website; and

115 (c) Notification to major statewide media.

116 (8) In the event a person provides notice to more than one thousand consumers at one
117 time pursuant to this section, the person shall notify, without unreasonable delay, the attorney
118 general's office and all consumer reporting agencies that compile and maintain files on
119 consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing,
120 distribution, and content of the notice.

121 3. (1) A person that maintains its own notice procedures as part of an information
122 security policy for the treatment of personal information, and whose procedures are otherwise
123 consistent with the timing requirements of this section, is deemed to be in compliance with the
124 notice requirements of this section if the person notifies affected consumers in accordance with
125 its policies in the event of a breach of security of the system.

126 (2) A person that is regulated by state or federal law and that maintains procedures for
127 a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or
128 guidelines established by its primary or functional state or federal regulator is deemed to be in
129 compliance with this section if the person notifies affected consumers in accordance with the
130 maintained procedures when a breach occurs.

131 (3) A financial institution that is:

132 (a) Subject to and in compliance with the Federal Interagency Guidance Response
133 Programs for Unauthorized Access to Customer Information and Customer Notice, issued on
134 March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit
135 Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift
136 Supervision, and any revisions, additions, or substitutions relating to said interagency guidance;
137 or

138 (b) Subject to and in compliance with the National Credit Union Administration
139 regulations in 12 CFR Part 748; or

140 (c) Subject to and in compliance with the provisions of Title V of the Gramm-Leach-
141 Bliley Financial Modernization Act of 1999, 15 U.S.C. Sections 6801 to 6809;

142

143 shall be deemed to be in compliance with this section.

144 4. The attorney general shall have exclusive authority to bring an action to obtain actual
145 damages for a willful and knowing violation of this section and may seek a civil penalty not to

146 exceed one hundred fifty thousand dollars per breach of the security of the system or series of
147 breaches of a similar nature that are discovered in a single investigation.

✓