STATE OF NEW YORK

1580

2017-2018 Regular Sessions

IN SENATE

January 10, 2017

Introduced by Sen. AVELLA -- read twice and ordered printed, and when printed to be committed to the Committee on Consumer Protection

AN ACT to amend the general business law, in relation to smart phone antitheft protection

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Legislative intent. The legislature finds that:

(a) According to the Federal Communications Commission (FCC), one in three robberies in the United States involves the theft of a mobile device, making it the number one property crime in the country. Many of these robberies often turn violent with some resulting in the loss of life.

(b) The FCC estimates that between thirty to forty percent of United States street theft involves a mobile device. In fact, more than forty percent of all robberies in New York city involve smartphones and other cell phones.

(c) Consumer reports projects that 1.6 million Americans had their smartphones stolen in 2012.

(d) According to the New York Times, one hundred thirteen smartphones are lost or stolen every minute in the United States.

(e) Major cities are home to the highest concentrations of cell phone theft, and officials in New York and California have been pushing for a cellphone kill switch in those states since April 2012. According to New York state attorney general, Eric Schneiderman, the United States Senate proposal would force the mobile industry to "stop dragging its feet and join us in protecting consumers."

(f) In April of 2012, U.S. senator Charles Schumer, D-New York, and New York city police commissioner Ray Kelly announced that the major U.S. cell phone carriers and the Federal Communications Commission have agreed to set up a national database to track reported stolen phones. Senator Schumer also introduced a bill called the mobile device theft

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD00862-01-7

deterrence act, which proposes a five-year prison sentence for tampering with the ID numbers of a stolen cell phone.

(g) According to press reports, the international trafficking of stolen smartphones by organized criminal organizations has grown exponentially in recent years because of how profitable the trade has become.

(h) Replacement of lost and stolen mobile devices was an estimated thirty-billion-dollar business in 2012 according to studies conducted by mobile communications security experts. Additionally, industry publications indicate that the four largest providers of commercial mobile radio services made an estimated seven billion eight hundred million dollars from theft and loss insurance products in 2013.

(i) Technological solutions that render stolen mobile communications devices useless already exist, but the industry has been slow to adopt them.

(j) In order to be effective, these technological solutions need to be ubiquitous, as thieves cannot distinguish between those mobile devices that have the solutions enabled and those that do not. As a result, the technological solution should be able to withstand a hard reset or operating system downgrade, and be enabled by default, with consumers being given the option to affirmatively elect to disable this protection.

(k) Manufacturers of mobile devices and commercial mobile radio service providers should make efforts to protect their customers from being targeted as a result of purchasing their products and services.

(l) It is the intent of the legislature to require all smartphones and other mobile devices offered for sale in New York to come with a technological solution enabled in order to deter theft and protect consumers.

§ 2. The general business law is amended by adding a new section 399-zzzzz to read as follows:

§ 399-zzzzz. Smart phone antitheft protection. 1. For the purposes of this section, "smart phone" means a cellular phone or other mobile device that: (a) is built on a smart phone mobile operating system; (b) possesses advanced computing capability; (c) enables network connectivity; and (d) is capable of operating on a long-term evolution network and successor wireless data network communication standards. Capabilities a smart phone may possess include, but are not limited to, built-in applications, internet access, digital voice service, text messaging, e-mail, and web browsing. "Smart phone" does not include a phone commonly referred to as a feature or messaging phone, a laptop computer, a tablet device, or a device that has only electronic reading capability.

2. Any new smart phone manufactured on or after July first, two thousand eighteen, sold or purchased in this state must be equipped with preloaded antitheft functionality or be capable of downloading that functionality. The functionality must be available to purchasers at no cost.

3. Wireless telecommunications equipment manufacturers, operating systems providers, and wireless telecommunications service providers shall either individually or jointly, by January fifteenth, two thousand eighteen, submit a report to the chairs and ranking minority members of the legislative committees with primary jurisdiction over telecommunication issues. The report shall describe the principal functions of a tool that manufacturers and operating system providers will utilize on new models of smart phones in order to comply with subdivision one of this section, and must describe the technology or functions included to ensure the baseline antitheft tool is easily operable by individuals with disabilities.

4. For the purposes of this section, the following terms shall have the following meanings:

(a) "CMRS provider" means a provider of commercial radio service, as defined in United States Code, title 47, section 332, and includes its authorized dealers.

(b) "Internet marketplace" or "online platform" means a digitally accessible platform that facilitates commercial transactions between buyers and community-rated sellers where the operator or the platform does not take possession of, or title to, the goods bought or sold.

(c) "Law enforcement agency" or "agency" means a duly authorized municipal, county, campus, transit, park, state, or federal law enforcement agency.

(d) "Repair and refurbishment program" means a program, offered by a CMRS provider, manufacturer, or retailer who is not primarily engaged in purchasing personal property of any type from a person who is not a wholesaler, through which used or previously owned wireless communications devices are restored to good working order.

(e) "Trade-in program" means a program offered by a CMRS provider, manufacturer, or retailer who is not primarily engaged in purchasing personal property of any type from a person who is not a wholesaler, pursuant to which used wireless communications devices are accepted from customers in exchange for either: (1) a noncash credit usable only for the purchase of goods or services from the CMRS provider, manufacturer, or retailer; or (2) a rebate from a manufacturer on the purchase of one of the manufacturer's wireless communications devices.

(f) "Wireless communications device dealer" or "dealer" means an individual, partnership, limited partnership, limited liability company, corporation, or other entity engaged in the business of buying or selling used wireless communications devices.

(g) "Wireless communications device manufacturer" or "manufacturer" means an individual, partnership, limited partnership, limited liability company, corporation, or other entity engaged in the business of manufacturing wireless communications devices.

5. (a) Every wireless communications device dealer, including an agent, employee, or representative of the dealer, but not an internet marketplace, shall keep a written record at the time of each purchase or acquisition of a used wireless communications device for resale. The record shall include the following and may be kept in electronic form:

(1) an accurate account or description of the wireless communications device purchased or acquired;

(2) the date, time, and place or the online platform the wireless communications device was purchased or acquired;

(3) the name and address of the person selling or delivering the wireless communications device;

(4) the number of the check or electronic transfer used to purchase the wireless communications device;

(5) the number of the seller's driver's license, New York state identification card number, or other identification number from an identification document issued by any state, federal, or foreign government if the document includes the person's photograph, full name, birth date, and signature; and

(6) a statement signed by the seller, under penalty of perjury, attesting that the wireless communications device is not stolen and is free of any liens or encumbrances and the seller has the right to sell it.

(b) Records required to be maintained under this subdivision shall be retained by the wireless communications device dealer for a period of three years.

(c) The record, as well as the wireless communications device purchased or received, shall at all reasonable times be available for inspection by any law enforcement agency.

(d) No record is required for wireless communications devices purchased from merchants, manufacturers, or wholesale dealers having an established place of business, but a bill of sale or other evidence of open or legitimate purchase of the wireless communications device shall be obtained and kept by the wireless communications device dealer, which shall be shown upon demand to any law enforcement agency.

(e) Except as otherwise provided in this subdivision, a wireless communications device dealer or the dealer's agent, employee, or representative may not disclose personal information received pursuant to paragraph (a) of this subdivision concerning a customer without the customer's consent unless the disclosure is made in response to a request from a law enforcement agency. A wireless communications device dealer shall implement reasonable safeguards to protect the security of the personal information and prevent unauthorized access to or disclosure of the information. For purposes of this paragraph, "personal information" is any individually identifiable information gathered in connection with a record under paragraph (a) of this subdivision.

6. A wireless communications device dealer, including an agent, employee, or representative of the dealer, shall not:

(a) make any false entry in the records of transactions involving a used wireless communications device;

(b) falsify, obliterate, destroy, or remove from the place of business the records, books, or accounts relating to used wireless communications device transactions;

(c) refuse to allow the appropriate law enforcement agency to inspect records or any used wireless communications device in the dealer's possession during the ordinary hours of business or other times acceptable to both parties;

(d) fail to maintain a record of each used wireless communications device transaction for three years; or

(e) purchase a used wireless communications device from a person under eighteen years of age.

7. A wireless communications device dealer shall pay for purchases of all used wireless communications devices by check mailed to a specific address or by electronic transfer.

8. (a) Whenever a law enforcement official from any agency has probable cause to believe that a wireless communications device in the possession of a wireless communications device dealer is stolen or is evidence of a crime and notifies the dealer not to sell the item, the dealer shall not: (1) process or sell the item; or (2) remove or allow its removal from the premises. This investigative hold must be confirmed in writing by the originating agency within seventy-two hours and will remain in effect for thirty days from the date of initial notification, until the investigative hold is canceled or renewed, or until a law enforcement notification to confiscate or directive to release is issued, whichever comes first.

(b) If a wireless communications device is identified as stolen or as evidence in a criminal case, a law enforcement official may:

(1) physically confiscate and remove the wireless communications device from the wireless communications device dealer, pursuant to a written notification;

(2) place the wireless communications device on hold or extend the hold under paragraph (a) of this subdivision, and leave the device at the premises; or

(3) direct its release to a registered owner or owner's agent.

(c) When an item is confiscated, the law enforcement agency doing so shall provide identification upon request of the wireless communications device dealer, and shall provide the name and telephone number of the confiscating agency and investigator, and the case number related to the confiscation.

(d) A wireless communications device dealer may request seized property be returned.

(e) When an investigative hold or notification to confiscate is no longer necessary, the law enforcement official or designee shall notify the wireless communications device dealer.

(f) A wireless communications device dealer may sell or otherwise dispose of the wireless communications device if:

(1) a notification to confiscate is not issued during the investigative hold; or

(2) a law enforcement official does not physically remove the wireless communications device from the premises within fifteen calendar days from issuance of a notification to confiscate.

(g) If a wireless communications device dealer is required to hold a wireless communications device at the direction of law enforcement for purposes of investigation or prosecution, or if the device is seized by law enforcement, the wireless communications device dealer and any other victim is entitled to seek restitution, including any out-of-pocket expenses for storage and lost profit, in any criminal case that may arise from the investigation against the individual who sold the wireless communications device to the wireless communications device dealer.

9. (a) Each wireless communications device dealer shall install and maintain at each physical location video surveillance cameras, still digital cameras, or similar devices positioned to record or photograph a frontal view showing a readily identifiable image of the face of each seller of a wireless communications device who enters the physical location.

(b) The video camera or still digital camera shall be kept in operating condition and must be shown upon request to a properly identified law enforcement officer for inspection. The camera must record and display the accurate date and time. The video camera or still digital camera must be turned on at all times when the physical location is open for business and at any other time when wireless communications devices are purchased or sold.

(c) Recordings and images required by paragraph (a) of this subdivision shall be retained by the wireless communications device dealer for a minimum period of 30 days and shall at all reasonable times be open to the inspection of any properly identified law enforcement officer.

10. A wireless communications device dealer, or the agent, employee, or representative of the wireless communications device dealer, who intentionally violates a provision of this section is guilty of a misdemeanor.

11. (a) This section shall not apply with respect to a wireless communications device returned to the store where it was originally purchased

pursuant to the return policies of the wireless communications device dealer, CMRS provider, manufacturer, or retailer.

(b) This section shall not apply with respect to wireless communications devices acquired by a: (1) CMRS provider as part of a trade-in or a repair and refurbishment program; (2) manufacturer as part of a trade-in program; or (3) retailer whose trade-in program: (i) reports to other national or regional transaction reporting database available to law enforcement; or (ii) reports as required by local ordinance.

§ 3. This act shall take effect January 1, 2018 and shall apply to smart phone sales made on or after that date.