Journal of Forensic & Investigative Accounting
Volume 10: Issue 2, Special Edition 2018

The Use of Zappers by Financial Terrorists

*By Hossein Nouri**

Terrorists need money to conduct their activities. They use various methods to finance their activities, including receiving money from individuals and countries sponsoring terrorist activities and obtaining cash through illicit business activities. For example, cigarette smuggling by purchasing them from a low tax state and selling them in a high tax state is used to fund terrorism. Erb (2013) notes that "high profile arrests in North Carolina, Michigan, and New York over the past decade have provided evidence that profits from cigarette smuggling were being diverted to fund terrorism. In at least one situation, the smuggler was paying for individuals to train with al-Qaeda."

According to Brightman (2009, p. 359):

> An ATF investigation initiated in 1996…involved a cigarette trafficking scheme in North Carolina, a low tax state, from which millions of dollars' worth of cigarettes were smuggled to Michigan, a high tax state. The defendants, twenty-five in all, were moving cigarettes by rental vehicles from Charlotte to Detroit to sell on the streets. Proceeds were then transferred by wire and by courier to bank accounts in Beirut, Lebanon. Portions of the proceeds were used to provide material support to the Hezbollah international terrorist organization in Lebanon.

In a similar way, zapper or phantom-ware software inadvertently creates opportunities for terrorists to evade taxation and gain profits. Because of the immense profits in illegal zapper use and low possibilities for getting caught, terrorists and terrorist groups can use zappers to fill their bank accounts.

Background and How Zappers Are Used to Falsify Data.

An automated sales suppression device, otherwise known as a zapper, is a software program that falsifies data regarding point of sale (POS) transactions. "Zappers alter the electronic sales records in a cash register (Furchgott, 2008)." They are computer functions or electronic components that facilitates tax evasion by altering or erasing sales transactions in POS systems, including electronic cash registers, which alter the reports produced by these systems. Zappers can be loaded on memory sticks, removable CDs, or USB keys. They can even be accessed through a link on the Internet (Martin and Berg, 2012). When the procedure is completed, the zapper is removed. Well-developed zappers leave no trace of the original data; everything is rewritten, and the program that did it disappears. The software often presents the perpetrator with two dialogue boxes: one reporting the day's sales total and another where the perpetrator enters the amount he or she wishes to hide. Zappers then compute which sales orders to hide and further suggests an amount of cash to take. Once identified, the software removes orders accordingly and renumber the remaining ones to ensure the removal is undetectable. If executed correctly, the business reports a lower sales total than its actual sales, and its cash total agrees to this lesser amount (Ainsworth, 2013).

Zappers also might completely remove cash bills. They consider excluded categories, renumber remaining bills, and generate a new control number for each transaction (Martin et al., 2012). Businesses who use zappers take extreme care to prevent evidence of its use. The original data, for instance, might be copied to a separate directory for modification. Following this treatment, the original data files are deleted and then replaced with the modified files. Essentially, the software creates two sets of books (Berg, 2014). Owners avoid sales taxes on the deleted receipts or items, while keeping these taxes collected from consumers and avoiding income tax. Because sales records are completely rewritten, even well-trained auditors may not detect this tax evasion. The software allows the owner of a business to alter the records to make it credibly appear that fewer transactions have occurred.

In the mid-1990s, a computer program became available that would "zap" sales transactions from POS systems or electronic cash registers (ECR). In 1996, Revenue Québec found the first zapper. Their use has become common because

*The author is a professor at the College of New Jersey

they are widely available, difficult to detect, and, most importantly, generate huge returns on minimal investments. Zappers cost around $500, and they can be directly installed into registers (Adams, 2012). Because most registers and POS software run on Microsoft Windows, zappers also can be installed into the cash register through an external USB drive, internet link, or removable compact disks. Zappers are relatively easy to use and have been more prevalent in smaller and medium-sized restaurants and stores. Because zappers are often run externally on a USB or hard drive, tracing the tampering of the register or sales software is difficult.

Zappers provide the opportunity to skim in a fully computerized environment by allows the business owner to operate in what appears to be a perfectly normal sales transaction. The use of this software allows the business owner to perform the electronic sales suppression at a convenient time, usually at the end of the business day, when the software systematically modifies the machine's transaction records to reduce the value of the day's sales (Pauli, 2013).

The idea of the zapping process is that cashiers record sales transactions and give customers the accurate receipts of goods or services during the normal day of business; however, at the end of the day, a portable USB device that contains the zapper is plugged into the register to remove the given dollar amount in sales from the day's receipts. To finalize this process, the zapper re-totals and recalculates the receipts, and the results are changes in the tax amount liabilities that the business owner is legally obligated to pay to the government or to other parties (e.g., a lessee). In some cases, the business using the zapper keeps two sets of records and books. One set of books is prepared for the tax authorities while the other set is for the business owner in case he/she decides to sell the company. Other statements show the real earning earnings of the business.

Types of Businesses Using Zappers

Zappers are used by cash-based businesses that record transactions electronically using a POS system, such as small restaurants, bars, retailers, gas stations, convenience stores, hair salons, dry cleaners, and grocery stores that have many cash deals/transactions. Businesses that are selling items that are levied with high excise taxes, such as gasoline, tobacco, or alcohol are much more likely to use zappers than other businesses. They are most common in small and medium-sized businesses in which there are usually fewer internal controls and most recorded transactions are paid in cash (Ainsworth, 2008a).

The main users of zappers are businesses located in a state in which there is sales tax. Zappers also are found in businesses all around the world, including Germany, Sweden, France, Brazil, Australia, and the Netherlands (Furchgott, 2008). While zappers are mostly used for skimming cash transactions, they also can be used for credit and debit card transactions (OECD, 2013). Zappers also are offered as a service. Under this approach, the company that installs the POS system for a business also offers to alter sales data by remotely accessing the point of sale system after installation.

Potential Use by Terrorists

As it becomes more difficult to transfer money between countries for terrorism, financial terrorists can use cash generated through zappers to fund terrorist activities. Since zappers hide cash transactions and are difficult to detect, financial terrorists can create a frontline cash business, such as a pizza shop, zap some cash transactions, and use the funds for domestic or foreign terrorist activities. Zapper software can give these frontline businesses an opportunity to illegally avoid taxes. Specifically, sales, income, corporate, payroll, and unemployment taxes can be lowered. Sales taxes are avoided since zappers are programmed to delete certain transactions. By not recording these transactions, a company's sales taxes are understated in the financial statements. Income and corporate taxes also are understated since transactions are not properly recorded due to the zappers deleting certain transactions (Ainsworth, 2008b). Unemployment taxes at both the state and federal levels are affected using zappers, as companies can use the cash saved from not recording transactions to pay employees under the table (Ainsworth, 2013). These tax savings can then be diverted to terrorist activities. For example, in a report of gas stations in Illinois, some stations had avoided as much as one million dollars in taxes (Lemov, 2012). Additionally, in Michigan, a chain restaurant owner was caught concealing up to $20 million in hidden sales using zappers (Sorge, 2013). In other words, since taxes are not paid properly by these businesses, funds diverted from the U.S. government can be funding terrorism.

Pervasiveness of Zapper Use and Governmental Actions

According to Ainsworth (2014), the amount of annual tax revenue lost "is estimated to cost state and local governments twenty billion dollars annually (two billion dollars in New York restaurants alone)." In a 2007 Detroit-area case,

investigators found that the owners of La Shish restaurant chain (thirteen restaurants) skimmed more than twenty million dollars in a four-year period and allegedly sent the money, using smaller cashier's checks, to Hezbollah in Lebanon (Ellison, 2012). In another situation, a local grocery chain associated with a dairy farm in Connecticut skimmed approximately seventeen million dollars over ten years using a zapper software system. The cash was received in large denomination bills and put into suitcases to ship to Saint Martin in the Caribbean. The audits of 2,000 cash-based businesses, including food stores, hairdressers, restaurants, and clothing stores in Sweden showed that sales transactions were underreported by about twenty to forty percent (OECD, 2013). Due to the difficulty of uncovering frauds involving zappers, there is problems in estimating the amount of cash skimmed and taxes lost, which leads to the contrast in estimates between sources. These findings show that the use of zappers is pervasive in cash-dominated businesses and can be used for terrorism.

To fight zappers in the U.S., many states with sales taxes have enacted laws to combat their use. Table I presents a list of twenty-five states with anti-zapper laws and details of legislation as of the end of 2017. Table II presents a summary of important features of each of the twenty-seven states' anti-zapper laws. [see Tables I and II, pgs. 218 and 220]

As shown in Tables I and II, while legislation varies state by state, legislative proposals generally aim to prohibit the possession or use of automated sales suppression devices, including zappers. The possession and use of zappers is considered a felony with fines and imprisonments in all states that have enacted laws against sales suppression software devices. Generally, states with a sales tax enact a law against sales suppression software devices. Five states without sales tax (Alaska, Delaware, Montana, New Hampshire, and Oregon) do not have an anti-zappers law since not much tax is lost by the use of zappers. Forty-six states and the District of Columbia levy a sales tax at the state and/or local level. Besides the twenty-seven states reported in Tables I and II, a few other states (Massachusetts, Missouri, and New York) have anti-sales suppression software device bills, which at the time of the writing of this paper, have not yet become law.

The lack of a national law against the use of zappers provides opportunities for financial terrorists to operate in states without anti-zapper laws and divert the skimmed cash for terrorism. Governments through other monitoring activities can prevent money laundering by terrorism. For example, the 2011 Patriot Act gives the U.S. government anti-money laundering powers to monitor financial institutions; however, the use of skimmed cash for homegrown terrorism is much more difficult to uncover. In addition, skimmed cash can now be moved through the new online payment systems, such as Bitcoin and other cryptocurrencies.

How to Detect the Use of Zappers

Detecting the use of zappers through conventional auditing techniques is difficult. Accounting ratios may remain coherent if purchases are made under the table. On rare occasions, zappers have been used to adjust inventory to cause purchases to match the amount of sales transactions actually recorded (Ainsworth, 2008c). When sales transactions are eliminated along with the related original purchase amounts, this process causes the gross profit percentage to remain the same. Therefore, it is extremely hard for auditors to detect zappers. The issue with detecting this form of fraud is that zappers overwrite the original entries in the company's books. Since the zapper eliminates the paper trail and the phantom-ware falsifies the accounting records, an auditor would have difficulty finding any falsification (Behlke, 2012).

Despite the difficulties in detecting skimmed cash through conventional methods, the following audit methods may help uncover the manipulation of transactions:

- compare financial ratios to industry benchmarks;
- use auditing software such as IDEA or ACL to recognize sales with unusual patterns;
- compare tip percentages to industry benchmarks for businesses with tips, which would have higher tip percentage payments unless they pay tips out of skimmed cash;
- inquiry of personnel for cash tip payments and reporting of tips in payroll;
- calculation of expected salaries and wages based on average hours and salaries, including tips, then comparison of expectations with business results;
- confirmation from suppliers about amount of transactions during the period and comparison to the books;
- increased training for auditors on the industry, ECRs, and POS systems; and
- education of auditors on how to find external (zappers) and internal (phantom-ware) devices.

In addition, these more unconventional methods should be used to fight these financial terrorists:

- obtain undercover footage of sales suppression in progress using IT solutions that are available to fight both traditional skimming and sales suppression devices;
- training specialized in the use of Computer Assisted Audit Tools and Techniques (CAATTs), such as SESAM, IDEA, and ACL;
- simultaneously examine all relevant taxes, such as income, sales, and payroll taxes;
- using the Net Worth and the Cash Deposit methods to uncover the reported income with lifestyle expenses;
- observe a day's transactions and comparing them with expected results;
- pose as a potential customer and later comparing the invoice received with the recorded amount; and
- train auditors to reprogram an ECR to reveal suppressed sales and transactions and print reports detailing these transactions.

How to Prevent the Use of Zappers Software

While the aforementioned techniques may detect the use of zappers and other sales suppression software devices, a better way to fight financial terrorism is to use prevention strategies, such as:

- mandate securing the integrity of stored data in electronic form, such as encryption and Standard Audit File-Tax (SAF-T) by manufacturers (Ainsworth, 2008b);
- certify cash registers as tamper-proof (Greece uses this policy before registers are sold) or replacing old registers that record transactions;
- introduce devices with remote access to registers for auditors;
- making business owners aware of the risk of being caught and promoting compliance through news media;
- securing sending transactional information to the auditor or Tax Authority;
- securing the integrity of electronically stored data in all ECR/POS (Electronic Cash Register/Point of Sale) systems; and
- enact a comprehensive federal law that makes it a felony to use sales suppression software, such as zappers.

Although these strategies may not stop the financing of terrorist activities, they can reduce it significantly if they are combined with frequent auditing of cash-based businesses.

Conclusion

This article discusses how financial terrorists—those who finance terrorist activities without being directly involved—can use sales suppression software devices such as zappers to skim cash from their frontline businesses and transfer those funds to terrorist organizations. As Nouri and Lafond (2012) note, Westerns countries, including the U.S., are generally reactive rather than proactive in proper security implementations. For example, additional security measures were put in place so that terrorists cannot have access to an airplane cabin after the bombing of Twin Towers. Other examples include asking airline passengers to take their shoes off to be checked after a shoe bomber attempted to explode an airplane and not allowing airline passengers to take liquids with themselves into the plane after a terrorist attempted to make bombs with liquids to explode the airplane. These examples show that after an incident happens, authorities attempt to put controls in place. This research suggests that since zapper software hides cash transactions and is difficult to detect, financial terrorists can create a frontline cash business, such as gas stations and pizza shops, zap some cash transactions, and use the funds for domestic or foreign terrorist activities.

This research takes a proactive view and suggests that, before the use of sales suppression software devices becomes widespread in frontline businesses to finance terrorist activities, the U.S. government should take appropriate steps by making them more difficult to use. This article discusses how zappers can be used to finance terrorist activities, their impact on tax evasions, and how to detect and prevent such activities. This research suggests that the federal government should create a law that prohibits the use of sales suppression software devices for cash-intensive businesses and mandate the use of "certified POS software" in which the system produces "encrypted sales data with digital signatures that validate a genuine transaction" (OECD, 2013).

References

Adams, G. (2012). State governments target tax-cheating software. *The Associated Press*. Retrieved 10/19/2016 from https://www.yahoo.com/news/state-governments-target-tax-cheating-185220977.html

Ainsworth, R.T. (2008a). Zappers—skimming cash with technology. *Proceedings of the Annual Conference on Taxation, 101*, 369–376.

Ainsworth, R.T. (2008b). Zappers and phantom-ware: a global demand for tax fraud technology. [Working paper]. *Boston University School of Law, Research Report No. 08-20.* Retrieved 12/30/2015 from https://www.bu.edu/law/faculty/scholarship/workingpapers/documents/AinsworthR060208.pdf

Ainsworth, R.T. (2008c). Electronic tax fraud: are there "sales zappers" in Japan? [Working paper]. *Boston University School of Law, Research Report No. 08-31*. Retrieved 12/30/2015 from https://www.bu.edu/law/faculty/scholarship/workingpapers/documents/AinsworthR102708.pdf

Ainsworth, R.T. (2013). Zappers and employment tax fraud [Working paper]. *Boston University School of Law, Research Report No. 13-3*. Retrieved 12/30/2015 from http://www.bu.edu/law/faculty/scholarship/workingpapers/documents/SSRN-id2207990zap.pdf

Ainsworth, R.T. (2014). Sales Suppression as a Service (SSaaS) and The Apple Store Solution [Working paper]. *Boston University School of Law, Paper 14–24.* Retrieved 12/31/2015 from http://www.bu.edu/law/faculty/scholarship/workingpapers/Ainsworth-SalesSuppression.html

Behlke, M. (2012). Tax Zappers. *National Conference of State Legislatures*. Retrieved 12/31/2015 from http://www.ncsl.org/ncsl-in-dc/publications-and-resources/tax-zappers.aspx

Berg, B. (2014). Zappers: what's new in electronic sales suppression [PDF File]. *Federation of Tax Administrators.* Retrieved 10/19/2016 from http://old.taxadmin.org/fta/meet/14tech/pres/berg_zappers.pdf

Brightman, H.J. (2009). *Today's White-Collar Crime: Legal, Investigative, and Theoretical Perspectives.* Routledge Taylor and Francis Group, New York, NY.

Ellison, G. (2012). New Michigan law cracks down on tax cheating "zapper" technology. *Michigan Live*. Retrieved 12/31/2015 from http://www.mlive.com/business/index.ssf/2012/08/new_michigan_law_cracks_down_o.html

Erb, K.P. (2013). Up in flames: cigarette taxes create opportunity for revenue and crime. *Forbes.* Retrieved 12/30/2015 from http://www.forbes.com/sites/kellyphillipserb/2013/08/20/up-in-flames-cigarette-taxes-create-opportunity-for-revenue-and-crime/

Furchgott, R. (2008). With software, till tampering is hard to find. *The New York Times*. Retrieved 12/30/2015 from http://www.nytimes.com/2008/08/30/technology/30zapper.html

Lemov, P. (2012). Sales tax zapped by Zappers. *Governing*. Retrieved 12/30/2015 from http://www.governing.com/columns/public-finance/col-sales-tax-zapped-tax-zappers.html

Martin, C. and Berg, B. (2012). Zap the Zapper: FTA. Technology conference and exhibition. *Federation of Tax Administrators*. Retrieved 10/19/2016 from http://old.taxadmin.org/fta/meet/12tech/pres/martin_berg.pdf

Nouri, H. and Lafond, C.A. (2012). Financial terrorists and the offshore outsourcing of tax return preparation. *International Journal of Critical Accounting (IJCA), 4(3)*, 272–282. Retrieved from http://www.inderscience.com/offer.php?id=47364

OECD (2013). Electronic sales suppression: a threat to tax revenues. *The Organization for Economic Co-Operation and Development.* Retrieved 12/31/2015 from http://www.oecd.org/ctp/crime/ElectronicSalesSuppression.pdf

Pauli, D. (2013). Business use fraud software for tax scam. *IT News*. Retrieved 12/30/2015 from http://www.itnews.com.au/news/businesses-use-fraud-software-for-tax-scam-339060

Sorge, R. (2013). Zappers. *The State of Texas Legislative Budget Board.* Retrieved 12/30/2015 from http://www.lbb.state.tx.us/Documents/Publications/Issue_Briefs/525_Zappers.pdf

Womble, S. (2015). The $20 billion tax fraud states are overlooking. *Boston University School of Law*. Retrieved 12/31/2015 from http://www.bu.edu/law/news/ainsworth_zappers.shtml

Table I: States with Anti-Zapper Laws as of December 31, 2017

State	Statute	Date of Law Enactment	Monetary Fine	Imprisonment	Subsequent Conviction	Device Confiscated?	Felony	Other Considerations
Alabama	§40-29-121	August 11, 2015	Up to $100,000 for individuals and $500,000 for corporation	1 year, 1 day to 10 years	1st :2–20 years 2nd:10–99 years or life 3rd:15–99 years or life	Yes	Class C	Liable for all taxes, fees, penalties, and interest
Arkansas	§5-37-505	August 15, 2013	Up to $10,000	3–10 years		No	Class C	Liable for all taxes, penalties, and interest
California	§7153.6 and §55363.5	January 1, 2014	Up to $5,000 for less than three and up to $10,000 for more than three devices	Up to 1 year, 16 months, or 2–3 years		No		Liable for all taxes, penalties, and interest
Connecticut	§12-428a	July 1, 2012	Up to $100,000	Up to 5 years		Yes	Class D	Liable for all taxes, penalties, and interest
Florida	§213.295	July 1, 2014	Up to $5,000	Up to 5 years		Yes	3rd Degree	Liable for all taxes, fees, penalties, and interest
Georgia	§16-9-62	May 3, 2011	Up to $100,000	1–5 years		Yes	Yes	Liable for all taxes and penalties
Illinois	§115/15	January 1, 2014		2–5 years, can be extended to 5–10 years		No	Class 3	
Indiana	IC 35-43-5-4.6	July 1, 2013	Up to $10,000	2–8 years		Yes	Class C	
Kentucky	§517.130	July 15, 2014	$1000 to $10,000	1–5 years		Yes	Class D	Permit revoked for 10 years
Louisiana	§47:1641.1	June 12, 2012	Up to $5,000	Up to 5 years, with or without hard labor		No		
Maine	17-A §909	September 1, 2012	Up to $5,000	Up to 5 years		No	Class C	
Michigan	§750.411w	April 1, 2014	Up to $100,000	1–5 years		No		Liable for all taxes and penalties
Minnesota	§289A.63	August 1, 2017	Up to $10,000	Up to 5 years		Yes		Liable for all taxes and penalties
North Carolina	§14-118.7	December 1, 2013	Up to $10,000	4–25 months		Yes	Class H	Liable for all taxes, fees, penalties, and interest
North Dakota	§12.1-23-16	August 1, 2013	Up to $10,000	Up to 10 years	Class A felony for the second offence. Also, subject to a civil penalty of up to $100,000	Yes	Class B	Assessed at double the amount determined that was evaded. Sales tax permit is also revoked, and a new permit cannot be obtained for a period of 10 years.
Oklahoma	§68-212.1	November 1, 2012	Up to $100,000	1–5 years		No		$10,000 administrative penalty for possessing the device. Sales tax permit is also revoked, and a new

								permit cannot be obtained for a period of 10 years.
Pennsylvania	§7268	July 13, 2016	Up to $5000 possessed not more than three automated sales suppression devices and up to $10,000 for more than three devices	Up to 3 years		No. It is considered a misdemeanor.		Liable for all tax, interest, and penalties. The penalties imposed by this section shall be in addition to any other penalties imposed by any provision of this article
Rhode Island	§44-19-42	July 1, 2014	Up to $50,000	Up to 5 years		No		Liable for all tax, interest, and penalties. Safe Harbor enacted.
South Dakota	§10-59-57	March 10, 2016	$10,000 for each return period, up to $120,000	5 years		Yes	Class 5	Liable for all tax, interest, and penalties
Tennessee	§39-14-704	July 1, 2012	Up to $100,000	1–6 years		Yes	Class E	
Texas	§326.001 and 326.002	September 1, 2013	Up to $10,000	6–24 months	2nd offence: 3rd degree felony punishable by two to ten years' imprisonment and a fine of up to $10,000	Yes	State jail	
Utah	§76-6-1301 to 1303	May 12, 2015	Up to twice the amount of the applicable taxes	Up to 5 years	Up to 15 years and $10,000	Yes	3rd degree	Liable for all tax, interest, and penalties
Vermont	Sec. 1. 13 V.S.A. § 2032	April 25, 2013	Up to $100,000	1–5 years		Yes		Liable for all tax, interest, and penalties. Safe Harbor enacted.
Virginia	§§58.1-1814 and 58.1-3907	July 1, 2014	$20,000	Up to 1 year		No	Class 1	Civil penalty of $20,000
Washington	§82.32.670	July 28, 2013	Greater of $10,000 or the amount of tax owed	Up to 5 years		Yes	Class C	Revocation of business license
West Virginia	§61-3-22a	June 8, 2012	$10,000 to $100,000	1–5 years		Yes		Liable for all taxes and penalties
Wyoming	§39-15-108	February 15, 2013	Up to $5,000	Up to 3 years		Yes	Tax evasion treated as separate offense	Liable for all tax, interest, and penalties

Table II: Summary of Enacted State Anti-Zapper Laws

State	ACT	Summary of Important Parts of the Law
Alabama	2015-502 (HB 18)	This act amends Section 40-29-119; adds Section 40-19-121; makes the possession or use of an automated sales suppression device, or phantom-ware, a Class C felony; punished by a fine of not more than $100,000, or $500,000 in the case of a corporation; the person is also liable for all lost revenue due the state and any locality; illegal activity includes knowingly selling, purchasing, installing, transferring, or being in possession of any automated sales suppression device or phantom-ware within the State of Alabama. http://revenue.alabama.gov/documents/executive/Current_Enacted_Legislation.pdf
Arkansas	1076 (SB 718)	Creates criminal and civil penalties for certain activities relating to software and other devices and mechanisms that modify or falsify electronic records for the purpose of evading taxes; amends Arkansas Code 5-37-101 to add definitions for devices or activities subject to penalty; amends Arkansas Code Title 5, Chapter 37, Subchapter 5 to add ACA 5-37-505 to define software and other devices and mechanisms used to falsify electronic records and the penalties if violated; amends Arkansas Code Title 26, Chapter 18, Subchapter 5 to add ACA 26-18-509, liability for payment of taxes and falsification of sales transaction records. http://www.dfa.arkansas.gov/offices/incomeTax/corporation/Documents/Corporate_Instructions_2013.pdf
California	AB 781 (Chapter 532)	Makes it a crime for anyone to knowingly sell, purchase, install, transfer, or possess software programs or other electronic devices that are used to hide or remove sales and to falsify records. Violators of this new law could be sentenced to up to three years in county jail, fined up to $10,000, and will be required to pay all illegally withheld taxes, including penalties and interest. https://www.boe.ca.gov/news/pdf/l369.pdf
Connecticut	135	Any person who willfully and knowingly sells, purchases, installs, transfers, or possesses any automated sales suppression device or phantom-ware shall (1) be fined not more than one hundred thousand dollars or imprisoned for not less than one or more than five years, or both; (2) be liable for all taxes, penalties, and interest due to the state as a result of such sale, purchase, installation, transfer, or possession; and (3) forfeit all profits resulting from the sale or use of such automated sales suppression device or phantom-ware. https://www.cga.ct.gov/2012/act/pa/2012PA-00135-R00HB-05421-PA.htm
Florida	2014-40 (HB 7081)	A person who violates this section: (a) commits a felony of the third degree, punishable as provided in s.775.082, s. 775.083, or s. 775.084. (b) is liable for all taxes, fees, penalties, and interest due the state which result from the use of an automated sales suppression device, a zapper, or phantom-ware. (c) shall forfeit to the state as an additional penalty all profits associated with the sale or use of an automated sales suppression device, a zapper, or phantom-ware. (4) an automated sales suppression device, a zapper, phantom-ware, or any device containing such device or software is a contraband article as provided in s. 932.701(2)(a) and may be seized and forfeited pursuant to the Florida Contraband Forfeiture Act. http://laws.flrules.org/2014/40
Georgia	HB 415/AP (Part II, Section 2-1)	(b) It shall be unlawful to willfully and knowingly sell, purchase, install, transfer, or possess in this state any automated sales suppression device or zapper or phantom-ware. (c) Any person convicted of a violation of subsection (b) of this Code section shall be guilty of a felony and shall be punished by imprisonment of not less than one nor more than five years, a fine not to exceed $100,000.00, or both. (d) Any person violating subsection (b) of this Code section shall be liable for all taxes and penalties due the state as the result of the fraudulent use of an automated sales suppression device or phantom-ware and shall disgorge all profits associated with the sale or use of an automated sales suppression device or phantom-ware. (e) An automated sales suppression device or phantom-ware and any device containing such device or software shall be contraband. http://www.legis.ga.gov/Legislation/20112012/116770.pdf
Illinois	HB 49	Any person who knowingly sells, purchases, installs, transfers, possesses, uses, or accesses any automated sales suppression device, zapper, or phantom-ware in this State is guilty of a Class 3 felony. http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=003501200K13
Indiana	1546 (Sections 42 and 43)	Defines "automated sales suppression devices," "phantom-ware," and related terms. Provides that anyone who knowingly or intentionally sells, purchases, installs, transfers, or possesses automated sales suppression devices or phantom-ware after June 30, 2013, commits unlawful sale or

		possession of a transaction manipulation device, which is a Class C felony. http://www.in.gov/dor/files/summary2013.pdf
Kentucky	13RD HB 185	Creates a new section of KRS Chapter 517 to prohibit the possession of an automated business record falsification device, commonly known as a tax zapper or phantom-ware; provide that possession of such devices is a Class D felony, and provide for the forfeiture of such devices and all proceeds associated with the sale or use thereof; amend KRS 139.760 to provide for a ten-year sales tax permit revocation whenever any permit holder uses an automated business record falsification device to violate any provision of the sales tax laws. http://www.lrc.ky.gov/record/13RS/hb185.htm
Louisiana	839 (SB 616)	Whoever violates the provisions of this Section shall be fined not more than five thousand dollars or imprisoned with or without hard labor for not more than five years, or both. https://legiscan.com/LA/text/SB616/id/655958
Maine	H.P. 1297 - L.D. 1764	A person is guilty of possession of an automated sales suppression device if the person sells, purchases, installs, manufactures, transfers, or owns any automated sales suppression device or phantom-ware. Possession of an automated sales suppression device is a Class C crime. http://www.mainelegislature.org/legis/bills/bills_125th/billtexts/HP129701.asp
Michigan	328 of 1931	(1) A person shall not knowingly sell, purchase, install, transfer, or possess in this state any automated sales suppression device or zapper, phantom-ware, or a skimming device. (2) A person who violates subsection (1) is guilty of a felony and shall be imprisoned for not less than 1 year or more than 5 years and, in addition, may be fined not more than $100,000.00. (3) A person who violates subsection (1) is liable for all taxes and penalties due the state as the result of the fraudulent use of an automated sales suppression device, phantom-ware, or a skimming device and shall disgorge all profits associated with the sale or use of an automated sales suppression device, phantom-ware, or a skimming device. http://www.legislature.mi.gov/(S(keb0wuyfi2exg412k1lswqyq))/mileg.aspx?page=getObjectandobjectName=mcl-750-411w
Minnesota		Sec. 2. Minnesota Statutes 2016, section 289A.60, is amended by adding a subdivision to read: Subd. 32. Sales suppression. (a) A person who: (1) sells; (2) transfers; (3) develops; (4) manufactures; or (5) possesses with the intent to sell or transfer an automated sales suppression device, zapper, phantom-ware, or similar device capable of being used to commit tax fraud or suppress sales is liable for a civil penalty calculated under paragraph (b). (b) The amount of the civil penalty equals the greater of (1) $2,000, or (2) the total amount of all taxes and penalties due that are attributable to the use of any automated sales suppression device, zapper, phantom-ware, or similar device facilitated by the sale, transfer, development, or manufacture of the automated sales suppression device, zapper, phantom-ware, or similar device by the person. Sec. 3. Minnesota Statutes 2016, section 289A.63, is amended by adding a subdivision to read: Subd. 12. Felony. (a) A person who sells, purchases, installs, transfers, develops, manufactures, or uses an automated sales suppression device, zapper, phantom-ware, or similar device knowing that the device or phantom-ware is capable of being used to commit tax fraud or suppress sales is guilty of a felony and may be sentenced to imprisonment for not more than five years or to a payment of a fine of not more than $10,000, or both. (b) An automated sales suppression device, zapper, phantom-ware, and any other device containing an automated sales suppression, zapper, or phantom-ware device or software is contraband and subject to forfeiture under section 609.5316. https://www.revisor.mn.gov/laws/?id=1andyear=2017andtype=1
North Carolina	SB 465	Offense: No person shall knowingly sell, purchase, install, transfer, possess, use, or access any automated sales suppression device, zapper, or phantom-ware. Penalty: Any person convicted of a violation of this section is guilty of a Class H felony with a fine of up to ten thousand dollars ($10,000). Liability: Any person who violates this section is liable for all taxes, fees, penalties, and interest due the State as the result of the use of an automated sales suppression device, zapper, or phantom-ware and shall forfeit to the State as an additional penalty all profits associated with the sale or use of an automated sales suppression device, zapper, or phantom-ware. Contraband: An automated sales suppression device, zapper, or phantom-ware, or any device containing such device or software, is contraband. http://www.ncleg.net/Sessions/2013/Bills/Senate/PDF/S465v4.pdf
North Dakota	SB 2126	Makes it illegal to sell, buy, possess, install, transfer, manufacture, own, or use an automated sales suppression device, zapper, or phantom-ware in North Dakota. These are programs which falsify electronic records, transaction data, or transaction reports of electronic cash registers and other point-of-sale systems. Individuals found in violation of this law would face a class B felony for the first offense, a class A felony for a second violation, and

		are subject to a civil penalty of not more than $100,000. https://www.ndchamber.com/capitolinsider/final-legislative-report/#.VobTlvkrLDc
Oklahoma	SB 1230 (Section 2)	B. It shall be unlawful to willfully and knowingly sell, purchase, install, transfer, or possess in this state any automated sales suppression device or zapper or phantom-ware. C. Any person convicted of a violation of subsection B of this section shall be guilty of a felony and shall be punished by imprisonment of not less than one (1) nor more than five (5) years, a fine not to exceed One Hundred Thousand Dollars ($100,000.00), or both. D. In addition to the criminal penalty provided in subsection C of this section, any person violating subsection B of this section shall be subject to an administrative fine of Ten Thousand Dollars ($10,000.00). Administrative fines collected pursuant to the provisions of this subsection shall be deposited to the General Revenue Fund. E. The Tax Commission shall immediately revoke the sales tax permit of a person who violated subsection B of this section. A person whose license is so revoked shall not be eligible to receive another sales tax permit issued pursuant to Section 1364 of Title 68 of the Oklahoma Statutes for a period of ten (10) years. http://www.oklegislature.gov/cf_pdf/2011-12%20INT/sb/sb1230%20int.pdf
Pennsylvania	Title 72 P.S. Taxation and Fiscal Affairs § 7268 and Pennsylvania Sales Tax Bulletin No. 16-001, 07/21/2016	(c)(1) Notwithstanding any other provision of this part, any person who purchases, installs, or uses in this Commonwealth an automated sales suppression device or zapper or phantom ware with the intent to defeat or evade the determination of an amount due under this part commits a misdemeanor. (i) Any person who, for commercial gain, sells, purchases, installs, transfers or possesses in this Commonwealth an automated sales suppression device or zapper or phantom ware with the knowledge that the sole purpose of the device is to defeat or evade the determination of an amount due under this part commits an offense which shall be punishable by a fine specified under subparagraph (ii) or by imprisonment for not more than one year, or both. A person who uses an automated sales suppression device or zapper or phantom ware shall be liable for all taxes, interest, and penalties due because of the use of that device. (ii) If a person is guilty of an offense under this paragraph and the person sold, installed, transferred, or possessed not more than three automated sales suppression devices or zappers or phantom ware, the person commits an offense punishable by a fine of not more than five thousand dollars ($5,000). (iii) If a person commits an offense under this paragraph and the person sold, installed, transferred, or possessed more than three automated sales suppression devices or zappers or phantom ware, the person commits an offense punishable by a fine of not more than ten thousand dollars ($10,000). http://codes.findlaw.com/pa/title-72-ps-taxation-and-fiscal-affairs/pa-st-sect-72-7268.html
Rhode Island	Section 44-19-42	Forbids anyone to sell, buy, install, transfer, or possess an automated sales suppression device or phantom-ware. Anyone who violates the law will be guilty of a felony and, upon conviction, will be subject to a fine of up to $50,000, or imprisonment for up to five years, or both. A person convicted under the law will also be liable to the State for all taxes, interest, and penalties relating to the person's use of such a device or program and will also have to disgorge all associated profits. http://www.tax.ri.gov/Tax%20Website/TAX/notice/Summary%20of%20Legislative%20Changes%202014.pdf
South Dakota	SL 2016, ch 69, §2, §4, and §5	54) It is unlawful to knowingly own, sell, rent, lease, purchase, install, transfer, possess, use, access, design, manufacture, or program any automated sales suppression device or phantom-ware. A violation of this section is a Class 5 felony. 56) In addition to any civil or criminal penalty, any person violating § 10-59-54 is liable for all sales and use tax, contractor's excise tax, or any other tax imposed by title 10, including any municipal sales and use tax, and all associated penalties and interest due the state as a result of the use of an automated sales suppression device or phantom-ware. 57) An automated sales suppression device or phantom-ware or any cash register or device containing an automated sales suppression device or phantom-ware is contraband and may be seized without a warrant by the secretary, agents or employees of the secretary, or any law enforcement officer of this state. The disposition of any property seized under this section shall be conducted pursuant to chapter 23A-37. http://sdlegislature.gov/statutes/Codified_laws/DisplayStatute.aspx?Statute=andType=Statute
Tennessee	HB 2226	(b) It is an offense for a corporation or individual to knowingly sell, purchase, possess, install, transfer, or use any automated sales suppression device, zapper, or phantom-ware. (c) A violation of subsection (b) is a Class E felony punishable by a fine only up to one hundred thousand dollars ($100,000). http://www.tn.gov/sos/acts/107/pub/pc0741.pdf
Texas	SB 529	Makes it a state jail felony to knowingly sell, purchase, install, transfer, or possess any automated sales suppression device or phantom-ware, including any device that contains a sales suppression device or a link to sales suppression software.

		http://www.legis.state.tx.us/tlodocs/83R/billtext/html/SB00529F.HTM
Utah	Title 76 Chapter 6 Part 13 Section 1303	(1) It is a third-degree felony to sell willfully or knowingly, purchase, install, transfer, use, or possess in this state any automated sales suppression device or phantom-ware with the intent to defraud, except that any second or subsequent violation of this Subsection (1) is a second-degree felony. (2) Notwithstanding Section 76-3-301, any person convicted of violating Subsection (1) may be fined not more than twice the amount of the applicable taxes that would otherwise be due, but for the use of the automated sales suppression device or phantom-ware. (3) Any person convicted of a violation of Subsection (1): (a) is liable for all applicable taxes, penalties under Section 59-1-401, and interest under Section 59-1-402 that would otherwise be due, but for the use of the automated sales suppression device or phantom-ware to evade the payment of taxes; and (b) shall disgorge all profits associated with the sale or use of an automated sales suppression device or phantom-ware. (4) An automated sales suppression device and any device containing an automated sales suppression device is contraband and subject to forfeiture under Title 24, Forfeiture and Disposition of Property Act. http://www.le.utah.gov/xcode/Title76/Chapter6/76-6-S1303.html?v=C76-6-S1303_2015051220150512
Vermont	H. 511	(b)(1) A person shall not knowingly sell, purchase, install, transfer, or possess an automated sales suppression device or phantom-ware. (2) A person who violates subdivision (1) of this subsection shall be imprisoned for not less than one year and not more than five years and fined not more than $100,000.00, or both. (c) A person who violates subdivision (b)(1) of this section shall be liable to the State for: (1) all taxes, interest, and penalties due as the result of the person's use of an automated sales suppression device or phantom-ware; and (2) all profits associated with the person's sale of an automated sales suppression device or phantom-ware. (d) An automated sales suppression device or phantom-ware and any device containing such device or software shall be deemed contraband and shall be subject to seizure by the Commissioner of Taxes or by a law enforcement officer when directed to do so by the Commissioner of Taxes. http://legislature.vermont.gov/assets/Documents/2014/Docs/ACTS/ACT013/ACT013%20As%20Enacted.pdf
Virginia	SB 611	B. Any person who willfully utilizes a device or software to falsify the electronic records of cash registers or other point-of-sale systems or otherwise manipulates transaction records that affect any local tax liability shall, in addition to any other penalties provided by law, be guilty of a Class 1 misdemeanor. C. In addition to the criminal penalty provided in subsection B and any other civil or criminal penalty provided in this title, any person violating subsection B shall pay a civil penalty of $20,000, to be assessed by the commissioner of the revenue and collected by the treasurer as other local taxes are collected and deposited into the treasury of the political subdivision of the Commonwealth served by the treasurer. https://lis.virginia.gov/cgi-bin/legp604.exe?141+ful+HB829ER2
Washington	SB 5715 – 2013-2014	Any person violating the provisions of this subsection, 37 including material breach of the monitoring agreement under (b)(iii) of SB 5715.PL p. 4 this subsection, is guilty of a class C felony in accordance with chapter 9A.20 RCW and, as applicable, (c)(ii) of this subsection. Any person violating the provisions of this subsection by furnishing an automated sales suppression device or phantom-ware to another person or by updating or repairing another person's automated sales suppression device or phantom-ware is, in addition to the punishments prescribed in chapter 9A.20 RCW, subject to a mandatory fine fixed by the court in an amount equal to the greater of ten thousand dollars, the defendant's gain from the commission of the crime, or the state's loss from the commission of the crime. For purposes of this subsection (4)(c)(ii), "loss" means the total of all taxes, penalties, and interest certified by the department to be due, as of the date of sentencing, as a result of any violation of the provisions of this subsection by a person using the automated sales suppression device or phantom-ware obtained from, or updated or repaired by, the defendant, which results in the defendant's conviction for violating the provisions of this subsection. http://lawfilesext.leg.wa.gov/biennium/2013-14/Pdf/Bills/Senate%20Passed%20Legislature/5715.PL.pdf
West Virginia	2012 SB 411; WV Code § 61-3-22a (2015)	Any person convicted of a violation of subsection (c) of this section is guilty of a felony and, upon conviction thereof, shall be confined in a correctional institution for not less than one nor more than five years, or fined not less than $10,000 nor more than $100,000, or both confined and fined. Any person violating subsection (c) of this section is liable for all taxes and penalties due the state as the result of the fraudulent use of an automated sales suppression device, zapper or phantom-ware and shall forfeit all profits associated with the sale or use of an automated sales suppression device or phantom-ware. An automated sales suppression device or phantom-ware and any cash register or device containing such device or software is contraband and, as such, subject to seizure and destruction by any duly authorized law-enforcement agency in the state, including the Criminal Investigation Division of

		the State Tax Department. http://www.legis.state.wv.us/wvcode/ChapterEntire.cfm?chap=61andart=3andsection=22A
Wyoming	SF 68	(ii) No person shall knowingly sell, purchase, possess, install, transfer, or use any automated sales suppression device, zapper, or phantom-ware; (iii) A violation of paragraph (ii) of this subsection shall be a felony punishable by a fine up to five thousand dollars ($5,000.00), or imprisonment for not to exceed three (3) years, or both. http://legisweb.state.wy.us/2013/Introduced/SF0068.pdf