The Coming Wave of Federal and State Tax Zapper Prosecutions:

Prosecuting Zapper Salespersons and Restaurant Owners While the Masterminds Go Free

*By Kirk C. Davis and Evan J. Davis**

Evan J. Davis and Kirk C. Davis examine computer software known as Zapper that facilitates tax cheats by electronically creating a second set of books.

1. Introduction

With a severely limited budget, and the same number of Special Agents as existed 50 years ago when there were 125 million fewer Americans, IRS Criminal Investigation does not need to look outside its own agency to find worthwhile, false-return and failure-to-file criminal tax cases to investigate.[1] This core group of tax cases in fact only accounts for about half of the IRS's inventory of criminal investigations, with the other half primarily made up of stolen-identity returns and money laundering cases frequently brought as part of a multiagency drug task force.[2] In such a resource-strapped environment, you wouldn't expect the IRS to be looking for yet another category of crimes to investigate.

But that's just what they are doing. With the help of IRS agents, federal and state prosecutions of persons filing false sales and income tax returns after having deleted or "zapped" sales have gone from one every five to 10 years, to one every few months within the past year.

This IRS has always prosecuted businesspersons who skim cash and maintain two sets of books—a real set and a second set without the skimmed cash used to report sales for income and sales tax purposes. What's different now is that the IRS is working hand-in-glove with state and local sales tax auditors and criminal investigators to target businesses, primarily restaurants, that use so-called zapper

KIRK C. DAVIS is in private practice in Seattle, Washington.

EVAN J. DAVIS is a Principal at the Beverly Hills tax boutique Hochman Salkin Rettig Toscher & Perez, P.C., focusing on civil and criminal tax and white-collar investigations, trials, and appeals.

software that suppresses or deletes cash sales, resulting in underreporting of sales tax.

Instead of just targeting the cash businesses that are zapping sales, the IRS and state investigators have finally turned their attention to the zapper salespersons and have trained agents to identify point-of-sale ("POS") data that have been erased by a zapper program. The John Yin zapper salesperson case discussed in detail below, which co-author Kirk defended, appears to be the first of its kind in the United States.

With the help of IRS agents, federal and state prosecutions of persons filing false sales and income tax returns after having deleted or "zapped" sales have gone from one every five to 10 years, to one every few months within the past year.

However, even with the additional focus on salespersons, those at the top of the pyramid—manufacturers of the zapper programs—have so far faced no repercussions. And technology will likely keep one step ahead of criminal investigators, so the masterminds of programs that enable tens of billions of dollars per year of tax fraud have little to worry about. It's again a story of the government plucking the low-hanging fruit while the more-difficult, and arguably more-worthy, cases go unworked.

2. What Is a Zapper and How Does It Work?

Cheating on taxes by keeping two sets of books is probably as old as taxes themselves. Before the advent of computerized POS systems, sales records were kept by hand or on cash-register tapes that had to be entered in a general ledger for later transmission to the government. Those who wanted to skim cash and underreport their sales and thereby reduce sales and income taxes had to keep a "fake" set of books/ledgers to provide to an accountant to prepare sales and income tax returns, and to the government in the unlikely event of an audit. These businesses would normally keep a "real" set of books to know their actual profit or loss. Equally important to many owners is that, without a "real" set of books, the owner would find it harder to know whether an employee is stealing cash. According to an Organisation for Economic Cooperation and Development ("OECD") report, the cash register was invented in 1879 to prevent employees from pilfering cash from his saloon.[3]

The defining feature of the low-tech version of cash skimming is that the business owner needs neither outside help to, nor an outsider to suggest, skimming cash.

Computerized POS systems transmit and store the cash-register-type data to a central program that allows for the easy transmission of sales information. With little more than the push of a button, came the ability to keep a second set of books electronically.

POS systems are more versatile than cash registers. Whereas in some businesses the person operating the till could simply pocket the cash and never enter information into a POS system, restaurants need to enter each order in the POS system because the POS system transmits food and drink orders to the kitchen and keeps track of what food and drink goes to what table. This means that restaurants, even those that skim, are forced to enter accurate information into their POS system. Cooking the books requires that the data be altered. But how?

There are low-tech and high-tech solutions to the problem of how to falsify the POS data. In the absence of a zapper, a restaurant owner could simply void entire tickets or portions of tickets where patrons have paid cash. Auditors would expect a certain level of voiding, and if the cash skim were small then an auditor might not conclude that the voided transactions included a cash skim. However, this approach is risky because anything more than a tiny cash skim would jump out at an auditor. Certain POS systems can be tweaked to prevent reporting of voided or refunded transactions on reports generated by the POS system, for example, but an auditor will easily be able to see that the POS system has been modified to avoid reporting these transactions.[4] The electronic breadcrumbs will lead the auditor right to the fraud, so cash skimmers look for a better, more high-tech solution. Further, the low-tech approaches can leave the restaurant vulnerable to embezzlement because employees can use the owner's skimming tools to skim for themselves.

The high-tech solution is to use a zapper program. Zapper programs are external programs, typically on a USB drive plugged into the POS computer, that delete sales data. As noted by the OECD, they are hard to detect because of their "sophisticated design and because the offending software is not present on the machine during normal use."[5] In the USB version of a zapper, the manager or owner possesses the USB device that contains the zapper program. Assuming he or she doesn't want others to be aware of the fraud, the manager will use the zapper at the end of the day or when others aren't looking to delete entire "tickets" paid in cash or percentages of cash tickets. Zapper developers have made the job easy for clients, trying to mimic the underlying POS software's interface and provide the manager options for deletions, such as clicking on items to delete, replacing higher-priced menu items with lower-priced ones, and even entering a total amount or percentage of cash sales to delete and allowing the zapper to choose how to achieve the result.[6]

Professor Richard T. Ainsworth, the nation's leading tax zapper expert and law professor at Boston University School of Law, describes the aspects of an "effective" zapper program: it not only deletes sales but it renumbers and recalculates records on each receipt, leading to altered data that look entirely consistent and reasonable to an auditor.[7] The best zapper, according to Ainsworth, will not just eliminate sales but will also delete inventory and employee time records to make the overall picture seem harmonious, as "it is hard to justify full inventory usage and a full complement of waiters in a restaurant that consistently reports less than a full volume of sales."[8]

Troublingly for auditors, more-recent POS systems permit online storage of sales data, which means that the zapper is also online and even more difficult to detect.

3. Scope of the Problem—21 Billion in Lost Sales Tax Revenue Annually

The Canada Revenue Agency has been one of the leaders in identifying the massive levels of fraud enabled by "zapper" software. A study completed in 2011 determined that up to one third of all of Canada's restaurants may be underreporting their income through the use of "zapper" software.[9] The Canada Revenue Agency has found an estimated $141 million in restaurant sales were erased by zapper technology.[10] The team of investigators found 143 cases of suspected fraud in restaurants with an average of $1 million in hidden or erased sales.[11] In some cases, the taxpayers were suppressing the sales and then using the money to pay the staff in cash.[12] The investigation found that the restaurants were in a type of arms race due to stiff competition. More and more businesses were feeling compelled to use the suppression software to compete with other restaurants.[13]

Although Canada's tax authorities recognized the problem of sales suppression software, they have not always been able to successfully combat it. A case in point is the British Columbia software company called InfoSpec[14] owned and operated by Pius Chan with assistance from his wife, Cindy Chan. InfoSpec was charged with fraud, four counts of evading income tax, and four counts of evading the Canadian Revenue Agency. They were convicted of fraud.[15] The Court noted that Pius Chan had "intended to defraud the public by providing or distributing a zapper program that allowed customers to suppress income and thereby evade tax."[16] In 2013, the conviction against InfoSpec was overturned on appeal because the Court said merely selling a product that the purchaser could use to commit fraud, the "zapper software," did not mean the company had committed fraud.[17]

In 2014, the loophole used by InfoSpec was closed when possession, distribution or sale of "zapper" software was made illegal.[18]

Quebec's tax authority estimates that in the 2007–2008 fiscal year, it lost $417 million in tax revenue from tax fraud in the restaurant sector alone.[19]

In 2012 in Illinois, a tax fraud investigation revealed that 27% of gas station operators had pocketed state and local sales taxes on gasoline over the four prior years. Some stations were skimming up to $1 million a year.[20]

Professor Ainsworth believes that the problem is costing states *$21 billion annually in the restaurant industry alone.*[21] Professor Ainsworth made his calculation-based study from the Canada Revenue Agency.[22] If one assumes that people in the United States eat out as much as people in Canada, then this estimate should hold true. In reality, the $21 billion figure underestimates the problem because that is only an estimate of the fraud going on in restaurants and does not account for other businesses that deal with a high percentage of cash customers.

The 2012 Illinois study of gas stations and the 2011 study of restaurants in Canada both showed that roughly 30% of businesses looked at were underreporting their income and in many cases using "zapper" software to enable them to do it efficiently and quickly.

Professor Ainsworth has said that the $21 billion figure very likely underestimates the losses to states.[23] He appears not to have estimated that loss in state income and sales taxes stemming from zapped sales, but in California, for example, the income tax rate can be as high as the sales tax rate—roughly 10%—and federal income tax rates can be nearly 40%, so the total tax losses from zappers could easily exceed $50 billion when all state and federal taxes are included.

4. Case Study—*J. Yin*

In early 2015, auditors from the Washington State Department of Revenue ("DOR") looked at the books of a restaurant called Facing East.[24] The auditors claimed it was a routine audit; however, many of the auditors from around the county had attended a Sales Suppression and Detection Techniques Symposium in partnership with the Federal Tax Administration on April 28 and April 29, 2014, in Pasadena, CA. Furthermore, in 2013, the Washington State Legislature outlawed the mere possession of sales suppression software.[25] So, it is clear, the agents from DOR were on heightened alert and primed to find evidence of sales suppression software.

Indeed, the true story of the investigation was later revealed in court documents filed by the U.S. Attorney's Office in the case of *J. Yin*.[26] It turned out that the auditors noticed a trend with restaurants that were using InfoSpec/Profitek POS systems.[27] The trend was that they were reporting unusually low cash sales.[28]

The pace of U.S. zapper prosecutions has picked up at both the state and federal levels.

At Facing East, auditors found telltale traces of the use of "zapper software." They noticed that the cash sales were at a flat 7% month after month, which was both low in comparison to other restaurants and unusually consistent for a restaurant.[29] It is more common for restaurants to have a higher percentage of cash customers in the range of 14–20% and for the percentage of cash customers to fluctuate from month to month.[30] This was a red flag to auditors from DOR who then sent in undercover agents to purchase meals in cash.[31] When the DOR auditors later ran an audit on Facing East and other restaurants using the Profitek POS system, they found that many of the undercover agents' meals they had paid cash for and kept receipts for had been "zapped" and were not recorded in the records of the business.[32]

When confronted with the disparity in the numbers and the zapped receipts, the owner of Facing East, Yu-Ling Wong, admitted to using the "zapper" software on a USB Flash Drive.[33] Ms. Wong then named John Yin as the person who had sold her the zapper software.[34]

John Yin was hardly a criminal mastermind. At the time he was prosecuted, he was 66 years old and had been supporting himself and his family in the United States by working as a dishwasher in restaurants.[35] After learning English, he went to community college to study computers. After he graduated from community college, he went to work for InfoSpec selling the Profitek POS system in 2008.[36]

Mr. Yin was assigned to a large portion of the Pacific Northwest to sell the legal Profitek POS system; however, he was told by Pius Chan and Cindy Chan to also provide the "zapper" software when restaurants requested it.[37] Many times restaurants would not buy the Profitek POS system unless it also came with the "zapper" software.[38] At first, the "zapper" was provided to the restaurants by USB flash drive; however, as the Internet access improved and "zapper" was outlawed in Canada, Mr. Yin merely provided an email address to restaurant owners so they could contact the Chinese manufacturers of the illegal software—the true masterminds of the fraud.[39]

Ms. Wong of Facing East was one of Mr. Yin's first customers for the Profitek POS system and the "zapper."[40] Ms. Wong had not even bothered to remove the USB flash drive from the POS system when she was being audited by agents of the DOR. IRS Special Agents then became involved in the investigation of John Yin and assisted with the DOR in setting up a sting operation to ensnare Mr. Yin. An undercover IRS agent posed as a restaurant owner from California who wanted to purchase the "zapper" software.[41] After Mr. Yin reluctantly agreed to sell the "zapper" software along with the legitimate Profitek POS system to the undercover agent, his home was searched pursuant to a search warrant.[42]

Mr. Yin was charged by Information with Wire Fraud in violation of Title 18 U.S. Code, Section 1343 and Section 2 and Conspiracy to Defraud the Government in violation of Title 18 U.S. Code, Section 371.[43] As in many of the cases discussed below, he was not charged with any Title 26 crimes, despite the central role that IRS agents played in the investigation.[44]

Mr. Yin negotiated a favorable guilty plea to the charges with substantial reductions in the government's original offer; however, at sentencing, the government was still recommending the low-end of the applicable guidelines at 46 months in prison.[45]

The defense successfully argued to the Court that Mr. Yin's conduct was not as egregious as suggested by the government and recommended supervision only.[46] The sentencing judge rejected the defense's suggestions that Mr. Yin had only a minor role and had not used sophisticated means to commit the offense, crediting the government's argument that he had provided the "zapper" to at least eight restaurants who had, in turn, evaded $3.45 million in taxes; however, the judge agreed the U.S. Attorney's 46-month sentencing recommendation was much too harsh and sentenced Mr. Yin to 18 months in prison.[47]

It does not appear that going after the restaurants is a priority of the local IRS office. Despite having gathered information about multiple restaurants that were using the "zapper" software from John Yin, the U.S. Attorney's Office has made no move to file criminal charges against any of the other restaurants. They have left that to state authorities to clean up. The only restaurant owner charged out of the investigation into John Yin was Ms. Wong, the owner of Facing East who was charged in Superior Court and received a non-custodial sentence. Presumably, all the other restaurant owners are being contacted by the DOR auditors and being asked to pay back taxes. Indeed, John Yin's restitution is being reduced as the back taxes from multiple other restaurants are paid by those owners. Ms. Wong likely is asking why she was singled out for different treatments than the other restaurant owners, some of whom also had sizeable cash skims.

Despite the best efforts of the U.S. Attorney's Office that issued a press release both when John Yin entered a guilty plea and when he was sentenced, there was surprisingly little local television coverage of his federal case compared to the state criminal case against the owner of the restaurant, Facing East.

However, John Yin's case received a lot of local, national and international attention.[48]

The Canadian press was interested because Pius Chan and Cindy Chan were, according to John Yin, providing restaurants with a way to obtain the illegal "zapper" software.[49]

Forbes also published an article on Mr. Yin's sentencing and added that a decade ago the IRS put into place its own software that compares cash to credit card ratios for business such as restaurants.[50]

The case even appeared in a publication in the United Kingdom.[51]

Presumably, the IRS will be encouraged by the press attention and see that further cases against salespersons will result in additional articles and, consequently, additional deterrence for both salespersons and business owners.

5. Zapper Prosecutions Have Finally Become Commonplace

Although it's difficult to learn about every case, it appears that Canada has prosecuted more zapper cases than the United States. Are Canadians simply more apt to skim cash? Unlikely. They simply got the jump on the United States, as did many other European jurisdictions. The United States is trying to catch up.

The pace of U.S. zapper prosecutions has picked up at both the state and federal levels. The first-known zapper case was the 1993 Stew Leonard's Dairy case in Connecticut, which involved a $17 million cash skim over 10 years using a customized zapping program.[52] The next federal zapper case was 13 years later, a tax-evasion prosecution against Talal Chahine in Detroit; Chahine allegedly zapped $20 million and sent the proceeds to Hezbollah in Lebanon.[53] Six years after Chahine, the IRS and various other state and federal agencies indicted a dozen persons for money laundering, arson, and immigration violations stemming from the owner of a handful of IHOP restaurants using a zapper program, burning down a restaurant, and hiring dozens of undocumented workers.[54,55] Four years later in 2016, Washington brought the Facing East and the Seattle U.S. Attorney's Office brought the John Yin cases discussed above. State taxing authorities brought three cases in 2017, with Connecticut charging Xioning Fan after a routine sales tax audit led to specially trained auditors to detect the zapper program, Illinois charging Sandra Sanchez after investigating her with IRS-CI, and Michigan charging Christina and Don Hyun Chan, owners of Sushi Samurai, after a joint investigation with IRS-CI. The common theme amongst the investigations is that the IRS rarely acts alone and, in contrast to the earlier zapper cases, frequently is brought in by state taxing investigators to help their investigations.

6. Going Forward, What Can We Expect?

Professor Ainsworth has been predicting and advocating that state and federal authorities would want to target cooperatively the tax gap including through training sessions such as the 2014 symposium in Pasadena California that appears to have yielded the 2016 Yin and Facing East prosecutions in Washington.[56]

In all but one of the recent cases, whether the case was prosecuted federally or by a state or local prosecutor, IRS Criminal Investigation was working hand-in-hand with other agencies. The authors are aware of one case that fits the same mold, with state and federal investigators assigned and of a similar investigation in a different state. At least half of the states have passed criminal laws specifically targeting zappers, so state authorities are well aware of the problem. Particularly in states that don't have an income tax, such as Washington, taxing authorities must be particularly vigilant to protect the public fisc.

One question is whether the trend of prosecuting zapper salespersons federally and the restaurant owners exclusively at the state level will continue. We both doubt it will. State sentences, at least the amount of time served, tend to be much lower than their federal counterparts. On the federal side, sentences exceeding 12 months require that a defendant serve at least 85% of the time imposed, and those 12 months and under must serve 100% of the time imposed. State sentences tend to have lower rates of time actually served, and that assumes that the court imposes any time at all. As seen in the Facing East prosecution, the one restaurant owner among the eight identified who was unlucky enough to be selected for prosecution received no time from the Superior Court judge. The IRS does not like to work on cases that result in no jail time, believing that the deterrence value of straight probationary sentences is insufficient to justify the IRS expending its scarce resources, so one should expect that the IRS will press for some federal prosecutions of restaurant owners as well as salespersons.

Keeping in mind the scarce resources and notwithstanding that neither the federal nor the state government appears interested in going after the other seven restaurants to which John Lin sold a zapper, the IRS likely will continue to see a benefit to work both the restaurant and salesperson zapper investigations. As happens with many federal investigations, the IRS will happily cede the laboring oar on much of the investigative work and focus on financial records analysis and calculations. By dividing the labor, the IRS can be a part of—and, therefore, claim credit for—a much higher number of investigations than if the IRS exclusively worked cases alone.

However, without putting more resources into suppliers and manufacturers of zapper software, which Canada and other countries have done, the IRS will still barely make a dent in the problem.

The bigger questions are will state governments follow the lead of other nations and require a technology fix to the problem such as real-time transmission of POS data to taxing authorities and will the IRS and other federal agencies reach for the higher-hanging fruit such as the wholesalers and manufacturers that cause substantially more harm than any single salesperson ever could? Even if most or all zapper manufacturers are based outside the United States, as Professor Ainsworth has noted, the government has tools including extradition and seizures that could upend the zapper market if the IRS and Department of Justice are willing to invest the time and money.

Based on past experience, only the low-hanging fruit should be worried.

ENDNOTES

* Kirk C. Davis specializes in personal injury and criminal defense. Prior to starting his own firm, he spent 15 years as a county and municipal prosecutor. He has handled several federal financial and tax cases including defending John Yin. Immediately before joining Hochman Salkin, Evan J. Davis spent nearly 20 years as a federal tax and white-collar prosecutor and civil tax litigator first in the Department of Justice Tax Division and then in the Central District of California in Los Angeles. Evan is Kirk's younger brother.

1 IRS: Criminal Investigation 2017 Annual Report, at *1 (available online at *www.irs.gov/pub/foia/ig/ci/2017_criminal_investigation_annual%20report.pdf*).

2 *See id.*; *www.irs.gov/compliance/criminal-investigation/enforcement-statistics-criminal-investigation-ci-enforcement-strategy*.

3 *Electronic Sales Suppression: A Threat to Tax Revenues*, OECD Report, 2013, at *9, available online at *www.oecd.org/ctp/crime/ElectronicSalesSuppression.pdf*.

4 *Id.*, at *14.

5 *Id.*, at *15.

6 *Id.*, at *16.

7 Richard Ainsworth, *Zappers—Retail VAT Fraud, International VAT Monitor*, May/June 2010, available online at *www.empcom.gov.in/WriteReadData/UserFiles/file/No.3%20A-5(1).pdf*.

8 *Id.*

9 *See* Dean Beeby Ottawa, *Taxman Finds Rampant Restaurant Fraud*, The Globe and Mail (Aug. 1, 2011), available online at *www.theglobeandmail.com/news/national/taxman-finds-rampant-restaurant-fraud/article2116523/*.

10 *Id.*

11 *Id.*

12 *Id.*

13 *Id.*

14 InfoSpec later became Profitek and now sells the Profitek POS systems.

15 *Information, State v. Wong*, No. 16-1-00179-0 (King Cnty. Sup. Ct. Wash. Feb. 5, 2016).

16 *Id.*

17 *Id.*

18 *Id.*

19 *See* Ryan Holeywell, *In an Uphill Battle, States Fight Tax "Zappers,"* Governing (Aug. 25, 2011), available online at *www.governing.com/blogs/view/uphill-battle-states-fight-tax-zappers.html*.

20 *See* Penelope Lemov, *Sales Tax Zapped by Zappers*, Governing (May 10, 2012), available online at *www.governing.com/columns/public-finance/col-sales-tax-zapped-tax-zappers.html*.

21 *See* Michael J. Bologna & Paul Shukovsky, *Tax-Zapping Software Costing States $21 Billion*, Bloomberg News (Sept. 15, 2017), available online at *www.bna.com/taxzapping-software-costing-n57982088046/*.

22 *Id.*

23 *Id.*

24 *Information, State v. Wong*, No. 16-1-00179-0 (King Cnty. Sup. Ct. Was. Feb. 5, 2016).

25 RCW 82.32.290(4).

26 Government's Sentencing Recommendation, DC-WA, 2:16-cr-00314 (Apr. 4, 2017).

27 *Id.*

28 *Id.*

29 *Information, State v. Wong*, No. 16-1-00179-0 (King Cnty. Sup. Ct. Was. Feb. 5, 2016).

30 *Id.*

31 Government's Sentencing Recommendation, *J. Yin*, DC-WA, 2:16-cr-00314 (Apr. 4, 2017).

32 *Id.*

33 *Information, State v. Wong*, No. 16-1-00179-0 (King Cnty. Sup. Ct. Was. Feb. 5, 2016).

34 *Id.*

35 John Yin's Sentencing Memorandum, *J. Yin*, DC-WA, 2:16-cr-00314 (Apr. 7, 2017).

36 *Id.*

37 *Id.*

38 *Id.*

39 *Id.*

40 *Id.*

41 Government's Sentencing Recommendation, *J. Yin*, DC-WA, 2:16-cr-00314 (Apr. 4, 2017).

42 *Id.*

43 Felony Information, *J. Yin*, DC-WA, 2:16-cr-00314 (Nov. 30, 2016).

44 Using mail or wire fraud instead of tax evasion not only exposes a defendant to a higher statutory maximum sentence, it can also increase his recommended sentence calculated under the U.S. Sentencing Guidelines.

45 Government's Sentencing Recommendation, *J. Yin*, DC-WA, 2:16-cr-00314 (Apr. 4, 2017).

46 John Yin's Sentencing Memorandum, *J. Yin*, DC-WA, 2:16-cr-00314 (Apr. 7, 2017).

47 Judgment, *J. Yin*, DC-WA, 2:16-cr-00314 (Apr. 14, 2017).

48 *See* Matt Day, *Seller of Software to Help Restaurants Hide Cash Sales Pleads Guilty*, The Seattle Times (Dec. 2, 2016), available online at *www.seattletimes.com/business/retail/seller-of-software-to-help-restaurants-hide-cash-sales-pleads-guilty/*; *see* Staff, *Salesman Who Targeted Asian Businesses Sentenced for Fraud*, Northwest Asian Weekly (Apr. 21, 2017), *http://nwasianweekly.com/2017/04/salesman-who-targeted-asian-businesses-sentenced-for-fraud/*; *see* Stuart Leavenworth, *That Sales Tax You Pay on Your Meal? Some Restaurants Keep It, Using Illegal Zappers*, Ledger-Enquirer (Dec. 6, 2017), available online at *www.ledger-enquirer.com/news/nation-world/national/article188196134.html*.

49 *See* Tom Blackwell, *Canadian Tax-Evasion Software Triggers Major US Probe and Leaves Salesman Facing up to 25 Years*, National Post (Dec. 11, 2016), available online at *http://nationalpost.com/news/canada/tax-evasion-software-triggers-major-u-s-probe*.

50 *See* Jay Adkisson, *Tax Zapper John Yin Gets Zapped by DOJ*, Forbes (Dec. 6, 2016), available online at *www.forbes.com/sites/jayadkisson/2016/12/06/tax-zapper-john-yin-gets-zapped-by-doj/#12f4e33429db*.

51 *See* Iain Thompson, *Bloke Sold Cash Register Code to Restaurants That Deliberately Hid Sales from Taxmen*, The Register (Dec. 5, 2016), available online at *www.theregister.co.uk/2016/12/05/point_of_sales_software_tax_fraud/*.

52 *S.J. Leonard, Sr.*, No. 3:93-cr-159 (D. Conn.).

53 *T.K. Chahine*, DC-MI, No. 5:06-cr-20248; Richard Ainsworth, *Zappers: Tax Fraud, Technology and Terrorist Funding*, State and Local Tax Lawyer (2008), at *2.

54 *K. Elkafarawi, et al.*, DC-OH, No. 3:12-cr-262.

55 A number of writers initially speculated that another case, against Chicago's informal "Mayor of Chinatown," Hu Xiaojun, aka Tony Hu., *Hu Xiaojun*, DC-IL, NO. 1:16-cr-00316, also involved a tax zapper. The sentencing memoranda instead suggest it was an old-fashioned skimming scheme in which Tony Hu physically altered paper records to then prepare false tax returns. One wonders whether the government would have caught Hu if he had been using a sophisticated zapper.

56 *Zappers: Tax Fraud, Technology and Terrorist Funding*, ABA Tax Lawyer: State and Local Edition, at *5.