

Boston University School of Law

Scholarly Commons at Boston University School of Law

Faculty Scholarship

6-2-2014

Sales Suppression as a Service (SSaaS) & the Apple Store Solution

Richard Thompson Ainsworth
Boston University School of Law

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship



Part of the [Banking and Finance Law Commons](#), [Business Organizations Law Commons](#), [Criminal Law Commons](#), [Law and Economics Commons](#), [State and Local Government Law Commons](#), [Taxation-State and Local Commons](#), and the [Tax Law Commons](#)

Recommended Citation

Richard T. Ainsworth, *Sales Suppression as a Service (SSaaS) & the Apple Store Solution*, (2014).
Available at: https://scholarship.law.bu.edu/faculty_scholarship/1432

This Working Paper is brought to you for free and open access by Scholarly Commons at Boston University School of Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarly Commons at Boston University School of Law. For more information, please contact lawlessa@bu.edu.



**SALES SUPPRESSION AS A SERVICE (SSAAS)
&
THE APPLE STORE SOLUTION**

Boston University School of Law Working Paper No. 14-24
(June 4, 2014)

Richard T. Ainsworth
Boston University School of Law

This paper can be downloaded without charge at:

<http://www.bu.edu/law/faculty/scholarship/workingpapers/2014.html>

SALES SUPPRESSION AS A SERVICE (SSaaS)
&
THE APPLE STORE SOLUTION

Richard T. Ainsworth

Zappers and Phantom-ware attract a lot of attention at tax fraud conferences.¹ However, in the world of sales suppression there seems to be something more – there is sales-suppression-as-a-service (SSaaS). A striking example of SSaaS may be unfolding in NY. The \$1 million sales suppression case against Congressman Michael Grimm (R-NY) appears to be a classic SSaaS case involving his Manhattan *Healthlicious* restaurant.²

SSaaS was the message of the keynote address at the California Board of Equalization's *Sales Suppression & Detection Techniques Symposium* in Pasadena California, April 28-29, 2014. SSaaS may be just as hard to detect as a Zapper or Phantom-ware programming, but it is much harder to localize. SSaaS providers are frequently remote and often act from across a border. Zappers and Phantom-ware at least have a physical presence in the location where the fraud is occurring.

The SSaaS mutation of traditional sales suppression appears to be a bigger problem in some parts of Manhattan than Zappers or Phantom-ware if we look closely at the undercover sting operations conducted by Tom Stanton and a cadre of confidential informants and investigators working for New York's Department of Taxation and Finance (NY-DT&F) in 2009.

Starting in Buffalo, NY in March, and ending in the Bronx by September, approximately 23 stings were set up by the NY-DT&F looking for Zappers and Phantom-ware. Sting locations were in Buffalo, Schenectady, Albany, Dutchess County, and the Bronx. False restaurants, manned by undercover agents, invited point of sale (POS) system salesmen to come in and demonstrate their wares. The clear theme rising from a review of about half of the sting transcripts is that while Zappers and Phantom-ware are readily available in New York, the preferred suppression technique is SSaaS. Twenty-two of the twenty-three salesmen that the NY-DT&F encountered offered suppression without prompting, but by and large it was SSaaS that the salesmen were pushing.³

¹ See: Richard T. Ainsworth, *Zappers – Skimming Cash with Technology: Are They in Use in New York?* 2009 EMPIRE STATE PROSECUTOR (Winter 2009) 11; *Zappers and Phantomware: The Need for Fraud Prevention Technology*, 50 TAX NOTES INT'L 1017 (June 23, 2008).

² Indictment, US v. Michael Grimm (ED NY, April 28, 2014).

³ John Crudele, *Today's Special: Scam dodges \$400M in Sales Tax*, NY POST (January 24, 2011) (discussing the early stings in Buffalo and referencing the Bronx stings with a notation that the undercover transcripts that were delivered to the NY DT&F were not being followed up) http://www.nypost.com/f/print/news/business/today_special_scam_dodges_in_sales_6PcQkUthfPabdCpDElx0XJ; John Crudele, *NY's sales-tax losses don't register*, NY POST 6 (January 16, 2014) (following up on the 2011 article, asking why nothing had been done about the undercover stings since, and indicating that he was talking with Tom Stanton) <http://nypost.com/2014/01/16/nys-sales-tax-losses-dont-register/>

In other words, the preferred way of suppressing sales was *not* to provide the proprietor with programming (a Zapper or Phantom-ware) to be *added to* a factory-ready POS system. The preferred way of suppressing sales was a *subtraction* method. SSaaS salesman offered to erase, delete, purge, crash or physically destroy a client’s hard-drive, and then replace it. The service was included in the price of the POS system. It was provided on demand or on a regular six-month schedule. The strategy was to leave the proprietor with “audit-proof deniability” for the missing hard drive. Sales records were instead kept in QuickBooks or on Excel spreadsheets – which were easily manipulated.

This paper recaps the author’s keynote address at the *Sales Suppression & Detection Techniques Symposium*.

The Tale of the Stings

Tom Stanton, the retired Director of Tax Enforcement for the NY-DT&F, provided the author with nine transcripts from undercover stings.⁴ Most of the locations released were from the Bronx/Manhattan area. The POS salesmen were from a range of providers.⁵ Three were small operators;⁶ one was medium sized;⁷ another three were reasonably large firms.⁸

The *Tale of the Stings* has five major threads, a disturbing conclusion, and a cutting-edge solution. The five threads focus on: (1) security – retail businesses want technology that protects against *employee* theft, (2) manipulation – retail owners also want technology that facilitates *employer* theft, (3) the Apple Store provides a business model that will resolve business concerns with security and government concerns with manipulation, (4) an analysis of NY’s suppression profile indicates that there are three dominant modes of suppression – Zappers, Phantom-ware and SSaaS, and (5) there is a strong movement by SSaaS providers to place a “second-set-of-books” in out-of-state storage.

The disturbing conclusions of this *Tale* are that there is mounting evidence that fraudsters are directly manipulating business data even while businesses are under audit, that the alleged sales suppression at *Healthalicious* could have been found and prevented by the NY DT&F if it had followed up on its stings, and that the same NYC fraud patterns can be found 600 miles away in North Carolina.

The elegant solution that comes from the *Tale* is that by adopting Apple Store management practice – encrypted security, storing transactional data in the cloud, and

⁴ The transcripts are numbered sequentially beginning with the first transcript delivered. The numbering has no other significance.

⁵ In 2 of the 9 transcripts it was not possible to determine the size of the firm.

⁶ There is a two employee firm, a five employee firm, and a firm with only forty clients, all in operating primarily in New York city.

⁷ One firm had four-hundred clients in Connecticut, New Jersey, and NY City.

⁸ One with thirty-five employees, 1,200 clients in NY city and two-hundred installations a year. It was within the top five for Aloha installations in the US; another firm had 1,100 NY city clients; a third was the top POS installer in Pennsylvania with forty employees in their NY office, and over 3,000 clients overall.

remote audit/ compliance – solves embezzlement and sales suppression. At the *Sales Suppression & Detection Techniques Symposium* the workability of this solution was demonstrated with Avatar⁹-DTI.¹⁰ Avatar-DTI is the cutting-edge sales suppression and missing trader¹¹ solution being implemented in many VAT jurisdictions. As a comparative tax policy matter, the Avatar-DTI/ Apple Store approach needs to be considered in the US retail sales tax.

(1) *Employee theft problems.* As a rule, the POS salesmen encountered in the NY stings opened their discussion of sales suppression by first assuring potential clients that their POS system was a highly secure, and an exceptionally accurate record-keeper that would protect against embezzlement.¹² Simplicity and security is the opening theme. This leads directly into SSaaS as the preferred suppression technique. The idea behind SSaaS is to defeat the POS completely, not defeat it on a piece-meal basis. Piece-meal vulnerability provides a window through which others (employees, or the POS system provider) can enter the system to do the same thing surreptitiously.¹³

In Transcript No. 3 two undercover agents discuss suppression with a salesman. The salesman has already suggested that SSaaS is the way to accomplish the agents' "goal," but the agents ask follow-up questions. They want to know if there is a way to do the same thing with internal programming. That is, without exporting data to Excel.

The salesman responds that no manufacturer would incorporate this kind of functionality directly in its POS equipment, or allow this kind of flaw, because it would make the system vulnerable to employee theft. The salesman then explains that the Aloha POS system "allows" manipulation through SSaaS, but that Aloha does not provide programming to do manipulation within their system.

⁹ Avatar Technologies Ltd, (www.avatar.ci) is based in Portugal. It partners with the Suisse group SGS - SOCIETE Générale de Surveillance and the South African GVG - Global Voice Group. Avatar's main activity involved the development and distribution of regulator-compliant products [electronic cash registers (ECRs); point of sale systems (POSs); enterprise resource planning systems (ERPs)] made by various manufacturers.

¹⁰ DTI – Data Tech International Ltd. (www.dti.rs) is based in Serbia. DTI's main activity is solution development and consultancy. It assists and advises governments combating tax frauds with commercially available technology.

¹¹ Missing trade fraud accounts for the majority of the €100 billion annual VAT losses in the EU. As a consequence, the EU has devoted considerable effort to coming up with technological solutions to it. Success in combating this fraud in the EU has been hampered not by the effectiveness of the solution, but by an inability to coordinate enforcement of the cross-border trade where this fraud is found in the VAT.

¹² NY Transcript No. 3 at 14-15 (discussing the high turnover in help in NYC restaurants because the staff is largely made up of artists or musicians, or people just passing through, and the fact that allowing these people access to cash and records is a vulnerability as well as a continual training requirement).

¹³ See, for example the case against the former owner of several subway restaurants in southern California. He pleaded guilty to a scheme involving gift cards and remote access to POS systems he had installed. Shahin Abdollahi and Jeffrey Wilkinson sold refurbished POS systems to Subway restaurants, and accessed the systems remotely to load value on to Subway gift cards after the stores closed. Jeremy Kirk, *Former Subway franchise owner pleads guilty to POS hacking*, NETWORKWORLD (May 14, 2014) available at: http://www.networkworld.com/news/2014/051514-former-subway-franchise-owner-pleads-281621.html?source=NWWNLE_nlt_afterdark_2014-05-15. See also: US Attorney's Office District of Massachusetts at <http://www.justice.gov/usao/ma/news/2014/May/AbdollahiShahinpleaPR.html>

Agent 1: So can I -- I mean if I have to export it to excel, is there anyway I can change the data in the program *without having to export it*?

Salesman: Well, not really because that -- nobody out there is really going to develop a product that does that. So, you need to accomplish the goal, and I know what your goal is.

Agent 1: Right.

Salesman: But you know, you can't make that a function of the application

Agent 1: Right.

Agent 1: -- for obvious reasons.

Agent 1: Right.

Salesman: And -- and even if you did, the trade off in that would be is that then *your system would not be very secure*. 'Cause then you could *potentially even have an employee* --

Agent 2: Yeah.

Agent 1: -- that can go in and do things --

Agent 1: Right.

Salesman: -- without you knowing, which you wouldn't want --

Agent 1: -- anyway.

Agent 1: And that's the thing. I mean if your not there 24/7, that could happen.

Salesman: So Aloha allows you to do it but, it -- it -- it doesn't make it, you know part of the application.

Agent 2: Right.

Salesman: Its not part of the Aloha application necessarily.

Agent 2: Right.

Salesman: So you're doing that in excel.

Agent 2: Exporting it to excel. Okay, that's fine.¹⁴

(2) *Employer theft facilitation – No law*. The sales pitch of the POS providers who were caught in the NY stings invariably relied on an assertion – there is no NY law (or DT&F regulation) requiring businesses to retain the *original electronic records* produced by their POS systems.¹⁵ The salesmen concede that there is a requirement to keep records, but they emphasize that it is *not* a requirement to keep POS records. A QuickBooks file or Excel spreadsheet pulled from a POS system is sufficient to satisfy the NY rules. If the QuickBooks or Excel files are subsequently manipulated and if the hard-drive of the POS happens to fail and needs to be replaced, that is not a concern of the POS salesman.¹⁶

¹⁴ NY Sting Transcript No. 3, at 61 (emphasis added).

¹⁵ Although NY has regulations dealing with record keeping that specifically includes POS systems, there is nothing in the regulation that mandates retention of original records in original digital form. A mandate like this would be unique in US tax law, and would require encryption. This kind of regulation is reasonably common outside the US. See: NY Department of Taxation and Finance, *Recordkeeping Requirements for Sales Tax Vendors*, Tax Bulletin ST-770 (TB-ST-770) June 2, 2011.

¹⁶ Some salesmen go so far as to say that they have no obligation to respond to any kind of third-party audit requests. See NY Transcript No. 7 at 25:

Agent 2: What [how] about this, what if somebody [performing an audit on us] contacts your company?

The obvious rejoinder to this argument, one that neither salesmen nor the undercover agents bring up, is that the absence of an affirmative requirement to preserve original records is not the same thing as a license to destroy them. This is the unstated understanding of each NY sting. It accounts for the salesmen's strong focus on the *service* nature of SSaaS. The premium service is a manual, hands-on service, not an automated, programmed service (although SSaaS can be performed remotely, and when it is there is no reliance on trace programming in the POS system). The objective is to delete with no record of it being performed. A complete destruction of the original POS data is professionally assured, "guaranteed,"¹⁷ and easily the best way to do this, is to completely replace the hard drive.

The salesmen profess to have no concern about tax fraud. Manipulation of POS records is so pervasive in the marketplace that 99.9% of businesses do it.¹⁸ The salesmen simply want to sell POS systems and provide professional-grade service. In fact, the largest of the providers caught in the NY stings *only* wanted to talk about services and came to the appointment without a system to demonstrate – needless to say, the undercover agents were surprised.¹⁹

Salesman: Never. We've never had it happen [in 15 years of business, see page 27].

Agent 2: (inaudible).

Salesman: Yeah.

Agent 2: Also that was another thing, I want to make sure, you know, if we get [an audit, and a request for data from your company].

Agent 1: *You would never comply?*

Salesman: Well, of course, *we don't have to comply.*

Agent 3: Okay.

Salesman: *We don't have to [comply with the requests of] Federal agents.*

¹⁷ NY Transcript, No. 5 at 20:

Agent: If I make any changes, does that stay on the system though?

Salesman: What do you mean?

Agent: I mean if you make any changes to the sales figures. Is there a record of that on the system on my hard drive?

Salesman: The record will be [gone]

Agent: Yes. The competitors they couldn't guarantee that.

Salesman: *We guarantee it.*

Agent: Okay. *So there is no past.*

Salesman: Correct.

¹⁸ NY Transcript No. 2 at 37:

Salesman: Ninety-nine point nine percent of all my customers [manipulate POS records].

Agent 1: Okay.

Agent 2: Oh, my god.

Salesman: Everybody's gotta do something, right?

Agent 1: There you go, right.

¹⁹ NY Transcript No. 3 at 4 (arriving without a system to demonstrate and wanting to simply talk about services); at 9 (indicating 1,200 NYC clients that their company follows whenever they expand with example of a Los Angeles, CA and a South Beach, FL expansion and installation going on at the time of the meeting); at 18 (indicating over 200 installations per year); and at 28 (indicating that they provide remote access to anywhere from the restaurants to the owner); at 29 (suggesting to the agents that they can do whatever they want with the data they download from the POS system); and at 31 (assuring the undercover agents that the suggested system, Aloha, would allow complete removal of data from the POS system without leaving a trace).

In fact, if the salesmen have a problem with their customers it is when the restaurant owners get records deleted without saving a copy on QuickBooks or a USB drive.²⁰ This appears to be why some POS salesmen are anxious to offer remote storage backup. “Remote,” in this instance means “out-of-state” storage. One salesman caught in the NY sting was receiving full daily reports from a client’s restaurant on his Blackberry and used it to explain to the undercover agents not only how his firm could remotely store data, but suggesting that this was how a secure second set of books could be aggregated.²¹

For example, in Transcript No. 1 the salesman illustrates his technical expertise in data recovery by describing how the Manhattan Prosecutor’s Office and the New Jersey State Police regularly call him as an expert in money laundering investigations. The implication is that he knows first hand how much data the authorities can recover from POS systems, and as a consequence his expertise could be very useful in suppressing

²⁰ Once the data is deleted it is gone. All the POS salesmen make this point, and make it repeatedly. This seems to be what makes the sale. For example see NY Transcript No. 7 at 30 (emphasis added):

Salesman: [The] end of the road [is] you determine [what] to submit. They're always going to come in and say hey, you're not counting tax right [correctly].

Agent 1: Right.

Salesman: Then you're going to get a reason for it but, you know, I have a customer come yesterday for [a] sales tax [audit] and he just didn't have his data from 2006. He lost his data for 2006. *Deleted it*. Did he copy it from a drive? He could have to a USB drive. *I'm like you're kidding, right? I just can't make this show up here. I have no magic for you, man, sorry.* So he's going to get hit with a (inaudible) backwards.

Agent 1: A no records kind of thing.

Agent 2: Right.

Salesman: (inaudible) and a loss of records. He's got physical--he's got a bunch of physical but he's missing some of the data. So he lost a lot of his physicals too but (inaudible), you know. *He goes can you help me retrieve the data, I go two days, I don't think so, man. I really don't.* I'll be honest with you. How long have you been having a problem? *I'll give you a letter. I'll give a letter saying you only have--you only keep three months of your data in the system, you know,*

²¹ NY Transcript No. 4 at 8-9:

Salesman: This is a customer of mine that allows me to show this. He's a customer of ours called ... , and what he does is every night, it comes right to his Blackberry. It comes to mine too, as well, too. Where you can see the reports get emailed when the stores closes. So it can come to your Blackberry, it can come to your email account, and the numbers will come up showing you, you know, what you did in cash, what you did in credit cards, what you did in voids. So you know, from one central location you'll be able to utilize that information.

Agent 1: Great. I think we need a system that really going to work for us.

Salesman: Uh-huh.

Agent 2: Say why do you -- why does he email them to you, just if you don't mind I ask?

Salesman: Just so I can show it as a demo thing.

Agent 2: Okay.

Salesman: Just show, “Hey, look. This is how it comes to my thing.” You know, just to kind of give you ar-- an idea. Here, I'll just open up one of the reports real quick. Let's see here, we'll do summary. Give me a second to open up my phone.

sales. The undercover agents expresses surprise at his willingness to assist with a criminal activity:

Agent 1: And you still -- you'll still delete our files for us even though you know it [will be destroying original evidence]?

Salesman: Excuse me?

Agent 1: You'll still delete our files for us knowing that [this is evidence that the tax authorities will be looking for] --

Salesman: Of course -- of course -- of course. Something like that, because you [know that is] what people in a lot of restaurants ask me? I just need you to know this. [It's] *no problem [for me]. It's your choice [not mine]*.

Agent 2: (Unclear).

Salesman: *There's no law* that says you have to keep [original POS system records]. *There is nothing that says that*.

Agent 1: I thought you had to keep records?

Agent 2: You don't have to keep records?

Salesman: No. QuickBooks. That's what you guys use QuickBooks for.

Agent 1: Right. Okay.

Salesman: That's why everything goes in. That's your inventory. *This [POS system] is not accounting software not -- accounting software*.

Agent 2: In other words, we can just steal some [cash] or hide some cash (unclear) --

Salesman: Yeah.

Agent 2: -- hide some cash -- through the system?

Salesman: The data is your data.²²

(3) *Apple Store solution*. The *no-law-prohibits-it* argument is persuasive. It appears to be a critical element in making the POS sales-pitch in the US. Around the globe (although not in the US) tax authorities have responded to sales manipulation by mandating that businesses adopt an *Apple Store business model* as a condition of getting a business license – real-time digital records, encrypted and stored in the cloud.

At the *Sales Suppression & Detection Techniques Symposium* the author asked the audience of 25 sales tax jurisdictions and IRS CI if anyone had audited and raised an assessment against an Apple Store? No one had, and no one knew of anyone who had.

The reason? The Apple Store has adopted a business practice of encrypting sales data and sending it to the cloud. It is a real-time, highly secure system.²³ Sales records are digitally preserved. There is never a question of whether or not a sale has been made, or if the appropriate tax has been collected and remitted.

²² NY Sting Transcript No. 1, at 34-35 (emphasis added).

²³ The details of the Apple Store security system are not readily available, and the statement in the text is based in part on hearsay pending confirmation from an official source.

Globally there are at least three variant versions of the *Apple Store solution*. One cannot help but think that if Steve Jobs were still with us that this would be the American solution to sales suppression, but currently there is none.²⁴ The three version of the *Apple Store solution* are:

- A government mandate requiring the use of government issued hardware, which includes proprietary encryption software. The government device is placed between cash terminals and receipt printers. A significant penalty is imposed when digitally-signed receipts are not issued. Encrypted records are stored locally. (Quebec solution).²⁵
- Government certification of encryption software developed by third-party providers that is mandated for use in a compliant (certified) hardware installation that is again installed between cash terminals and printers. Use is a condition of business licensure (Rwandan, Swedish, and Belgian solutions). Some versions store data centrally (Rwanda) while others store data on site (Sweden and Belgium). Penalties apply for not issuing a receipt.
- Government mandate of encrypted transmission (SIM cards and/or cable) of all transactions in real-time to a government “fiscal cloud” with the dedicated device as an option to serve some business needs (Ivory Coast solution). Penalties apply for not issuing a receipt.

Because a true *Apple Store solution* is currently under implementation in the Ivory Coast – the Avatar/DTI model – a solution that includes cloud storage of encrypted transactional data – the author secured permission to demonstrate the creation, encryption, and digital signing (from the Ivory Coast tax administration servers) of a receipt drafted in California. This process took less than three seconds. The encrypted data was remotely capture (in the Ivory Coast), and was then accessed (from California) and audited (during the presentation by the author) from the back end of the dedicated Ivory Coast tax authority’s “cloud.” The decryption and remote audit of the transaction took a minute.

Because an *Apple Store solution* is not in place in New York (or in any other state in the US) the POS salesmen encountered in the NY stings were able to sell their systems as highly secure from *employee* theft, but highly vulnerable to *employer* manipulation.

(4) *NY’s Zapper and Phantom-ware profile*. The NY stings also uncovered Zappers and Phantom-ware applications. The salesmen discouraged their clients from using them, and strongly recommended the SSaaS service model.²⁶ Zappers and Phantom-ware were considered too complicated. The real reason my have had more to do with the salesmen wanting to secure follow-on business as a restaurant expanded to

²⁴ Richard T. Ainsworth, *California Board of Equalization, Sales Suppression & Detection Techniques Symposium* (April 28, 2014) powerpoint slides, at 27.

²⁵ The Quebec solution was demonstrated at the *Sales Suppression & Detection Techniques Symposium* by Daniel Prud’homme, Vice President for Revenue Quebec.

²⁶ The sting transcripts released did not include the Schenectady stings where reportedly the NY DT&F found Zappers that the local POS salesmen called “the key.” This term does not appear in any of the transcripts the author has had access to.

other locations,²⁷ or as indicated above some of the POS salesmen may have had other scams going on with gift cards and need access for these reasons.²⁸

The nine transcripts released fall into three groups. In some there is no Zapper or Phantom-ware references, in others there are Zappers or Phantom-ware applications offered, but in the largest group there is a strong push for SSaaS as other methods are explained and then discounted.

No Zappers & No Phantom-ware

At one extreme is the salesman in Transcript No. 2. The undercover agents set up a discussion by asking the salesman if he can provide them with a Zapper, or Phantom-ware application and the response is that there is nothing like that available. There is only manipulation-as-a-service.

Agent 1: The question is this, you say that if we make, like, a weekly basis \$10,000 cash --

Salesman: Uh-huh.

Agent 1: -- we'd like to go to the other numbers instead of 10,000, we'd like to --

Salesman: *Bring it down?*

Agent 1: Bring it down *for bookkeeping and accounting* -- accounting, let's say 5,000, right?

Salesman: Well --

.....

Agent 1: *Is there anything that you can give us*, like, for back office where this will be in the front and this will be in the back?

Salesman: Oh, no.

Agent 1: No?

Salesman: *I can manipulate it.*

Agent 1: Uh-huh.

Salesman: I can manipulate. It's called -- three things very careful with this.²⁹

Zappers

The salesman in Transcript No. 8 takes a different approach to this issue. He does not offer a Zapper for sale, but instead puts a price on manipulation-as-a-service – \$65 per hour for a three-hour service call every six months.

It is not clear who will make the service call. It could an associate or the salesman himself, but in all probability the person doing the service will be in possession of a Zapper that is custom designed to work with the specific POS system being sold. It

²⁷ See: NY Transcript No. 3 at 9 (indicating that this salesman has clients in NYC that are expanding with their services in Los Angeles, CA and South Beach, FL); NY Transcript No. 4 at 10 (indicating that this salesman installs for an 800 store gourmet sandwich shop that is opening 4 or 5 new shops per week with their POS services).

²⁸ See the trials of Shahin Abdollahi and Jeffrey Wilkinson, *supra* note 13.

²⁹ NY Transcript No. 2 at 20 (emphasis added).

is highly unlikely that any \$65 per hour technician could reconstitute six months of transaction records in the manner offered in three hours of manual manipulation.

The only way to do this kind of detail-specific manipulation is with a Zapper. This is perhaps the most interesting part of Transcript No. 8. The salesman captured in this sting most certainly has a Zapper, but he is unwilling to transfer it to the restaurant owner. The preference to sell a service (SSaaS) is underscored.

Salesman: So let's--you're saying you want to take cash out of the cash drawer but not let the system know? ... Yes, there is a way to do it... But [to do] that you have to manage--, we have to do it in the database; we have to change the database. And that [is something] we would not [do] in this part, in the front end of the program.

Agent 2: Is that difficult or straight-forward?

Salesman: A little bit difficult, not like, not something that's like really simple but it would require something like not.

Agent 2: Reprogramming?

Agent 1: Do you charge extra for that?

Salesman: Yes, we would. We have to charge extra. ... *Well, we would have to do it.* We would have to do it like, let's say every half a year you [will] want to do it, so you call us, we come in--

Agent 1: Right. How long would it take?

Salesman: That way we charge by the hour. Like \$65 for the hour. take no more than three hours at max.³⁰

Phantom-ware

Transcript No. 6 discusses Phantom-ware, and the application is reasonably common among the salesman's associates. It has even acquired the nick-name of the Wizard, or the Wizard Wand. It is a database management tool. The tool is not original equipment, but is added to the factory-finished POS system by technology people at the salesman's company.

Agent 1: Wow. So, going back to the reports, one of my concerns is being able to adjust the report.

Salesman: Okay.

Agent 1: *So I don't have to fully report all the cash.*

Salesman: Oh, oh, no. Yeah. You're--no. It's called--you would use what's called the database management tool.

Agent 1: Okay.

Salesman: That's what it's called. We call it the Wizard. The Wizard Wand.

Agent 2: Wizard Wand.

Agent 1: Excellent.

Salesman: And you kind of like, you've got your transactions.

Agent 2: Mm-hmm.

³⁰ Transcript No. 8, at 9-10.

Salesman: And if there's transactions you don't want there, and the logo in the software, and *it's something we only put on if you request it.*
Agent 2: Okay.³¹

What follows next in the transcript is really quite extraordinary. The salesman explains that the Wizard is custom made, and will be designed to meet the specific needs of the business purchasing the POS system.³² It involves having one-on-one discussions with the owners of the company. The offer comes with a very clear warning that when the restaurant activates this Phantom-ware application that data deletion will be complete and irreversible. The client is warned that he needs to back up data to an Excel spreadsheet or QuickBooks in case of an audit.

Salesman: And you would actually come into the office and talk to like some of the owners of our company.

Agent 1: Okay.

Salesman: They'll sit down with you and they'll decide--you'll tell them how you want to do stuff.

Agent 2: Okay.

Salesman: And then *they'll actually set you up with the way you're going to--your whole process works.*

Agent 2: Okay.

Salesman: Because *once you delete stuff it's gone.* You can't bring it back.

Agent 1: Right.

Agent 2: So it's, it's off the hard drive, everything.

Salesman: *It's, it's gone. Like it does not exist anywhere.*

Agent 2: Is there any way to save it or no?

Salesman: Yes. You can save it on like--you can export like a back-up file to like a laptop or something, or a flash drive.

Agent 2: Okay. Personal.

Salesman: So you would take a backup, a duplicate system image.

Agent 1: Right.

Agent 2: Right.

Salesman: Take that and then do your thing, on your actual POS.

Agent 2: Gotcha.

Agent 1: Right. Because--I mean, *for the ST100, for the tax, the sales tax, I obviously don't want to report all the--*

Salesman: *Yeah. Every restaurant does it.*³³

³¹ NY Transcript No. 6 at 32 (emphasis added).

³² The implication is that the salesman's firm will manufacture the Wizard for each business that purchases a system. The custom design of the Wizard has apparently something to do with the specifics of the particular business, so it is not a "one-size-fits-all" Wizard, nor is it a Wizard manufactured or provided by the POS manufacturer. The Wizard is part of this salesman's service contract.

³³ NY Transcript No. 6 at 32-33 (emphasis added).

Later on in Transcript No. 8 it becomes apparent that the Wizard is a major selling tool for this firm. They seem to have locked up most of the Thai restaurants in NYC by sheer word of mouth.

Salesman: You actually need--you actually would need like--you actually need to *have a program installed on a laptop*, and take your laptop in, and it's like, and change your database. Aldelo [is the best POS for this] --

Agent 1: So I'm--

Salesman: That's why a lot of like Thai restaurants use it. And that's why a lot of small restaurants--

Agent 2: Which kind of restaurants?

Agent 1: Thai.

Salesman: *Like we have lots of Thai restaurants.*

Agent 2: Oh, Thai restaurants. They like Aldelo 'cause it's (unclear).

Salesman: Oh, *they love it. Yeah. Yeah, they love it. They put it in every single place and it's like--and they call all their friends. We have like 150 Thai restaurants in the City.*

Agent 1: I guess they're all doing the same with their cash.

Salesman: And here's the thing is that a lot of them don't really want to spend money on a POS.

Agent 2: Mm-hmm.

Salesman: But then they call their friends and they're like, you know, which POS should I get? I think I'm just going to get like one from the food distributor, or whatever.

Agent 2: Right.

Salesman: They just want to order them, like whatever one that the distributor sends them. And their friends are like, no no you know, you need, you need to go with Aldelo. *Here's why. And it's because it boils down to based our service.* Like, they never have to worry about anything.

Agent 2: Right.

Salesman: *If they have a problem they call.* They like it.

Agent 1: I suppose unless from--you know, *like an audit point of view they could come and take everything and there's no record of--*

Salesman: There's none. It doesn't--I mean, there's--it doesn't exist.

Agent 1: Right.

Salesman: It's all gone.

Agent 1: And that's my biggest worry.³⁴

(5) *Out-of-State Records.* A final characteristic of the sales pitches made by the POS salesmen captured in the NY stings is that SSaaS services commonly include an offer to store accurate records (the second set of books) in a remote location. Frequently storage is across state lines leaving only the manipulated records at the restaurant. A jurisdictional boundary becomes an audit barrier.

³⁴ NY Transcript No. 6 at 59-61 (emphasis added).

Out of state storage of POS records makes it very difficult for state auditors to follow the data trail. Even if an auditor suspects that the POS provider may be holding a second set of books for a period of time, the fact that they are in another state creates a barrier.

Perhaps the Pennsylvanian POS salesman in Transcript No. 4 provides the best example. He received daily downloads of client data on his Blackberry handset that duplicated the records sent to the owner. The context suggests that the client would manipulate the data (and save it), the business location (in NYC) would delete it completely, and the salesman (in Pennsylvania) would keep a true record until it was no longer needed.³⁵

The salesman in Transcript No. 1 came to NYC from his headquarters in New Jersey. The salesman in Transcript No. 3 worked out of the Manhattan office of a firm that had 1,200 clients in NY, but 3,000 nationally and followed their clients as they installed systems in Los Angeles, California and South Beach, Florida.³⁶ Fully remote access was provided to the POS systems at all locations. This salesman explained how to remotely delete records in the Aloha POS system they specialized in providing.³⁷ This firm also seemed to prefer to work with franchises.³⁸

Transcript No. 5 presents a discussion between a POS salesman and several undercover agents about remote manipulation of the Aldelo and Micros POS systems.³⁹ The salesman explains that they will access the POS system remotely along with the owners to help with manipulation, if necessary.⁴⁰ Transcript No. 6 involves a firm that is active in Connecticut, NY and New Jersey specializing in remote services and training. For the Aldelo system it prefers, this firm is willing to enter into pure service contracts for owners who buy their systems over the internet. Once again, this market in NYC is saturated with service providers.

Agent 1: Right.

Salesman: We actually end up--we have a lot of calls from people that say hey, I have Aldelo but it's not really working. It seems like it should be working better. *So what we do is we re-program the database and then we go and do all the training.*

Agent 1: Right.

Salesman: And then people sign up for support (unclear).⁴¹

The danger with having a POS provider with remote access, who possesses original records and who knows that records are manipulated, is that a state auditor will demand access. In Transcript No. 7 the undercover agents present exactly this issue to a large POS provider. This topic comes up after the salesman explains that it is highly

³⁵ NY Transcript 4 at 8-9 and *supra* note 21.

³⁶ NY Transcript 3 at 36.

³⁷ NY Transcript 3 at 31.

³⁸ NY Transcript 3 at 44-46.

³⁹ NY Transcript 5 at 18-19 & 21.

⁴⁰ NY Transcript 5 at 71.

⁴¹ NY Transcript 6 at 16 (emphasis added).

unlikely that state auditors would have the expertise to determine that records have been deleted on POS systems. But, what if they did, and what if they asked? First of all, the salesman had never heard of this kind of audit inquiry in 15 years of work in the POS business, and even if it did occur his company would not comply with the demand, *because there is no law* requiring these records to be held, and certainly no law requiring them to allow access.⁴²

Tale of the Stings
A Disturbing Set of Conclusions

When fraud becomes prevalent in a market-place, and when enforcement is lax, fraudsters become brazen. Perhaps it comes from an excess of confidence in the technology, or perhaps it comes from the general hubris that criminals seem to have, but brazen suppression fraudsters have shown up on both sides of the Atlantic Ocean when technology is employed to assist in suppressing sales.

Direct audit interference. The Dutch case of the Grand Café Dudok is an example of a brazen suppression fraud.⁴³ It is hard to imagine a more over-the-top fraud than when an active audit is going on in one room of a taxpayer's business, and a cash register salesman is called in to conduct sales suppression training sessions to employees in an adjoining room. Hubris is "over-the-top" when, as in this case, the training session is directed precisely (and knowingly) at defeating the ongoing audit. The Dutch case preserves much of the judicial outrage, and is worth reading.

Astonishingly, Transcript No. 5 presents exactly the same case as the Grand Café Dudok, but the scene is set in NYC not Amsterdam. In this transcript the salesman is

⁴² See NY Transcript No. 6 at 25, *supra* note 16.

⁴³ LJN: AX6802 (Jun 2, 2006) (in Dutch). Dudok skimmed cash receipts with a primitive zapper and used a portion of the cash to pay employees under the table. The Belastingdienst (Dutch IRS) was suspicious of the low wages reported, and thought that additional (unreported) compensation might be being distributed (under the table). Testimony in the case indicated that on the second day of the payroll audit the managing director of Straight Systems BV visited Dudok where he was approached by the Dudok's owner-manager. Straight Systems BV supplied the Finishing Touch point-of-sale cash registers that were used by Dudok. The owner-manager explained that he was having difficulty accounting to the Belastingdienst for the wages that were being reported, in part because the auditors were also questioning the turnover that was reported. The numbers did not "seem right" to the auditors, and they were requesting back-up data, something that would lead them to the primitive zapper he was using.

The managing director of Straight Systems explained the existence of a more sophisticated zapper, a "hidden delete" option already embedded in the Finishing Touch cash registers. This was, "... a hidden menu option that, after enabling ..., allowed operators of catering establishments to delete cash register receipts from the system." [LJN: AX6802, at Consideration of the Evidence (Jun 2, 2006) (in Dutch)]⁴³ After this discussion "... an employee of [Straight Systems] visited [Dudok] and explained [and enabled] the application of the erase rule [or hidden delete function], after which [Dudok] subsequently decided to start using [it] ..." [LJN: BC5500, at F3].

The case discusses three software programs: Twenty/Twenty; Finishing Touch; Tickview.exe. Twenty/Twenty was a US touch-screen program that did not have a phantom-ware application. Straight Systems BV added the phantom-ware application to Twenty/Twenty and renamed the program Finishing Touch. Using just this program you can view the sales ticket and change data. With a secret command the Tickview.exe program within Finishing Touch can be activated and the operator is asked if they would like to delete the whole ticket. If an affirmative response is given then the system records a "no sale" and the entire audit trail to the original data is eliminated.

demonstrating a system and comes to a point in the demonstration where the point he is making is exactly what was done two weeks earlier to help a client under audit.

Salesman: Man to man.

Agent 1: Okay.

Salesman: (inaudible) two months ago.

Agent 1: Two months ago.

Salesman: *They were being audited.*

Agent 1: *They were being audited.*

Salesman: Yes, they have like three restaurants.

Agent 1: Oh, they have three now? Okay.

Salesman: So they call us.

Agent 1: Is it Italian?

Salesman: No.

Agent 1: Okay.

Salesman: It's American.

Agent 1: Okay.

Salesman: We had a few of those though based out of Connecticut *but our guys run down, they spoke to the manager; this is how you do it.*

Okay?

Agent 1: Okay.

Salesman: Basically you want the back office feature.

Agent 1: Right.

Salesman: Sales basically filter out (inaudible) timeframe.

Agent 1: Timeframe, exactly.

Salesman: Okay. There's some dollar amount and basically it watches that or reconfigures the information you want it to report.

Agent 1: Right.

Salesman: You can configure the reports for the information you want for your accountant to report.

Agent 1: Report, right. Okay.

Salesman: You know, just keep in mind --

Agent 1: Did they have any problems after that?

Salesman: -- it's fine.

Agent 1: It's fine. Okay.

Salesman: We got this request. We honor it generally. We don't usually do it ourselves.

Agent 1: Right.

Salesman: The liability issues.

Agent 1: Right.

Salesman: But we show you the proper way.

Agent 1: Right.

Salesman: In terms of the data being (inaudible). You have to make sure that your inventory information corresponds with your ordering, \$10,000 liquor.

Agent 1: Right. We talked about that.

Salesman: You know what I'm saying. Then your report shows you're

only selling \$5,000 of liquor.

Agent 2: Right.

Salesman: You've got on hand of inventory or you have to watch it.

Agent 1: How do you deal with that?

Salesman: Well basically you've got to make sure -- I don't have the exact answers to that.

Agent 1: Right.

Salesman: Our guys would be able to direct you in terms.⁴⁴

The above exchange occurs at page 15 of the transcript. The salesman does not leave until page 49. It is very clear from the text that the undercover agents wanted to know the name of the restaurant where this POS firm compromised an active audit. The salesman is careful not to reveal too much, and this gets the agents working overtime. After the Salesman leaves the undercover agents start sorting through all the clues.

Agent 2: I want to say probably Hard Rock Café or -- no, that's too big.

Agent 1: Yes, Jesus, something like that. It's got to be an independent with three locations. Midtown, three locations, big.

Agent 2: I used to live up here.

Agent 1: And then what we can do is -- you used to live up this way?

Agent 2: Yes, in Manhattan. I lived near Broadway.

Agent 1: We can always have investigators go in and see what system they have and if he has that system, then it's one of his clients. You know what I mean?

Agent 2: Right, right.

Agent 1: If he has an Action system and it's a big restaurant and they have three locations, it's got to be it, right?

Agent 2: Yes, yes, exactly.

Agent 1: And if they had a recent audit, (inaudible) audit.

Agent 2: Yes.

Agent 1: We can run that and say it's a recent audit and it's got his system and has three locations then we've narrowed it down. We know about which restaurant it is.

Agent 2: And then you guys can do an investigation on that?

Agent 1: Well yes. *He just said we changed their records because they were under audit.*

Agent 2: Wow.

Agent 1: *We changed their records because they're under audit.*

Agent 2: Yes.

Agent 1: *And everything went fine.* So, yes. That's why when they engage you like that they don't want to give you the names. You try to get as much information as you can.⁴⁵

Reportedly, the NY DT&F never followed up on the lead provided by the undercover sting. It is not clear to this author why this is the case, but there could have

⁴⁴ NY Transcript No. 5 at 13-15.

⁴⁵ NY Transcript No. 5 at 50-51.

been compelling reasons not to follow through (we simply do not know). The reasoning however, is not apparent from the transcripts nor is it explained in conversations with the NY DT&F.

Hubris at Healthalicious. The NY stings are a window into sales suppression fraud in NYC in the 2009-2010 time frame. They predict the kind of “over-the-top” hubris that the indictment suggests was rampant at *Healthalicious*.

The indictment against Michael Grimm was ironically unsealed in NY at the same time this presentation on SSaaS was delivered in Pasadena, CA (April 28, 2014). This coincidence is matched by another – the NY stings were an ongoing operation set right in the middle of the indictment’s tax years – 2008, 2009, and 2010.⁴⁶ As a result, the NY stings provide a comprehensive looking at the sales suppression environment within which the alleged sales suppression took place at *Healthalicious*. They inform any good understanding of Michael Grimm’s case. For example, Exhibit Item B in the case is the hard drive that was removed from the POS system in the *Healthalicious* restaurant.⁴⁷

It is very possible that some of the same POS systems and salesmen could well be involved in the Grimm case and in the stings.

Duplication in North Carolina. But there is more. 600 miles south of NYC, in September of 2010 a small partnership of two women opened a wine bar in reasonably large city in North Carolina. One partner installed an Aldelo POS system, and with the help of the installer secured remote access to the system, manipulated sales, and then embezzled cash from the partnership. After reading about Zappers, Phantom-ware and sales suppression on the internet, the other partner made contact in 2012.

It took four years to bring this private fraud case to resolution. The partnership is now dissolved, and all back taxes have been paid. The embezzling partner is gone, and the remaining owner summarizes the events as follows:

Ok, this is what I discovered. There is a program in the Aldelo POS, that [name omitted] referred to, that enables you to void cash sales. I know that this is happening in [my town] due to my conversation with [Name of business omitted] on front street...basically, they alluded to having two sets of books and using this program. [Name omitted] didn’t find it on my system, but I believe it was accessed via LogMeIn, which doesn't leave an audit trail. Sounds crazy, but once I got a court injunction and disabled LogMeIn my cash sales and deposits increased. My discount usage went down, ect. My [Aldelo] sales rep [name omitted] tried on numerous occasions to come in and update LogMeIn and I told him that he would be in contempt of court if he touched my system. He also went on affidavit defending my biz partner, stating that the system was not running on unverified files and that the reports were not manipulated. When I talked

⁴⁶ US v. Michael Grimm, *Indictment* (Doc. 1) No. 1:14-cr-00248-BMC-RML (E.D. N.Y. April 25, 2014).

⁴⁷ US v. Michael Grimm, *Discovery Letter & Attachment to Discovery letter* (Docs. 14 & 14-1) No. 1:14-cr-00248-BMC-RML (E.D. N.Y. May 19, 2014) at Discovery Exhibit B and Item 25.

to Aldelo, they told me my program was outdated and that the reports should match. Which they did not according to my math. When I look at a comparative analysis since I have had control of the books over the last 6 months, the cash sales received is drastically different. Before, we were within dollars of par level in till. And now I have 100's of dollars in deposits.⁴⁸

Remarkably, this North Carolina fraud is a carbon copy of the fraud that the salesman discussed in NY Transcript No. 6 at 59. The use of LogMeIn⁴⁹ to gain remote access to an Aldelo POS was explained by the salesman in Transcript No. 5 at 18.

However, it is equally possible to travel about 600 miles due west of NYC to the Toledo, Ohio area where seven I-HOP restaurants were also found engaged in the same fraud.⁵⁰ Instead of using LogMeIn the owner of these franchises used Team Viewer software to gain remote access, and manipulate the installed POS system.⁵¹ In this instance the POS system was a newly installed advanced-level MICROS system that I-HOP Corporate had mandated for all franchise operations so that it could assemble accurate data at the corporate head quarters in Glendale, California.⁵² In the IHOP case the manipulation of sales not only reduced tax obligations it reduced the local franchise fee due.⁵³

Our question is: Why do we find the same fraud in North Carolina and in Ohio that we find in NYC? Why can we go 600 miles south of NYC, find the same Aldelo POS, the same remote manipulation of records through LogMeIn, and the same system vulnerability exploited by a salesman/ installer? Why is the only difference when we travel 600 miles west of NYC is not the fraud, but the substitution of Team Viewer for LogMeIn remote access software, and substitution of a MICROS POS for the Aldelo POS?

The answer is that SSaaS fraud is bigger than NYC. The way SSaaS fraud is carried out is not specific to the access technology or the POS system deployed. SSaaS has entered the blood stream of American retail business. This is the way business is done (unfortunately) in far too many places in the US. Thus, the NY stings tell a story that is bigger than the frauds in NYC alone.

⁴⁸ Personal e-mail, May 20, 2014 (on file with author).

⁴⁹ The LogMeIn program is commercially available. See: <https://secure.logmein.com>.

⁵⁰ See: Indictment at ¶¶ 46-54, notably ¶47, United States of America v. Tarek Elkafrawi et. al. N.D. Ohio, Case No. 3:12cr 262. Richard T. Ainsworth, *Zappers & Employment Tax Fraud* - a paper for IRS/State Workforce Agencies Conference (BU School of Law, Law and Economics Research Paper No. 13-3 (January 28, 2013) available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2207990.

⁵¹ The Team Viewer program is commercially available. See: <http://www.teamviewer.com/en/index.aspx>

⁵² The IHOP franchise consists of approximately 1,522 domestic and international restaurants. In 2010 IHOP Corporate ordered the legacy SABLE POS system to be phased out, and replaced with a state of the art MICROS POS system.

⁵³ The fees included a royalty payment of 4.5%, and advertising payment of 3% (2% local, 1% national), rent (a set amount or 8% of net sales; whichever is greater) and various franchise fees or equipment lease payments.

Avatar-DTI
The Apple Store Solution in Operation

The key to preventing sales suppression fraud is to obtain secure, encrypted transactional sales data from the moment of a sale. This is the *Apple Store business model*. The most advanced solution on the market today for accomplishing this was demonstrated at the California Board of Equalization's *Sales Suppression & Detection Techniques Symposium* – the Avatar-DTI system that is currently being installed in the Ivory Coast.

The Ivory Coast is mandating that all businesses must adopt secure POS systems as a condition of licensure. Avatar-DTI provides this security by creating an invoice (receipt) in a Certified Invoicing System,⁵⁴ and then immediately transmitting this data⁵⁵ to a VSDC (Virtual Sales Data Controller) server within the tax administration. The VSDC produces a digital signature that is returned to the point of sale terminal for replication on the invoice (receipt) and for retention in the tax administration's records server (along with the basic data of the transaction itself). To be valid an invoice (receipt) must include this signature.

Through the signature an auditor can match documents from the point of sale with the transactional records within the tax administration. The Certified Invoicing System (provided to the author for demonstration purposes) will generate fully compliant returns, analyze business data, and create reports for the taxpayer if needed. Enforcement by the tax administration will involve digital matching of taxpayer-generated documents (receipts/invoices and returns) as well as taking steps to ensure that taxpayers use these secure devices whenever they make sales.

There will be no suppression fraud in the Ivory Coast soon. The jurisdiction will become an Apple Store thanks to Avatar-DTI.

Similar security systems are in place in Quebec, Belgium, Sweden, and Rwanda but the Ivory Coast system is the most advanced and least expensive on the market today. In the early days of government-required, encryption-based security for POS systems these modules were costly. The Quebec modules cost \$800 per cash register, and the mandate to adopt these measures in Quebec was so expensive that the government had to subsidized the purchase.⁵⁶ In contrast, the total out-of-pocket cost for the Avatar-DTI system is approximately \$200 per device. In cases where a business would prefer to lease the device and accounting package the charge is less than \$1 per day.

⁵⁴ Certified Invoicing System (CIS) – any electronic cash register, any terminal with cash register software, any computer (POS) using cash register software, or any other similar system that can be used for registration of outbound transactions in accordance with the standards provided by a governing regulatory authority.

⁵⁵ Using SSL (Secure Sockets Layering) protocol.

⁵⁶ Revenue Quebec unveiled its plans for the MEV pilot project (scheduled to begin in late 2009) in January 2008. A prototype was demonstrated at the Federation of Tax Administrators Annual Conference in Denver, Colorado on June 2, 2009. Physically, the MEV looked like a relatively small 2 x 1 x 6 inch metal box that was connected to the printer and the ECR by standard cables.

At the *Sales Suppression & Detection Techniques Symposium* a test transaction was entered into an Avatar-DTI device. Data was sent to the Ivory Coast VSDC, and a receipt was printed in California with the encrypted signature (three seconds). Then the tax administration's dedicated server in the Ivory Coast was accessed, the receipt was found, and it was verified. Later, data was altered in the Ivory Coast server, and the receipt was checked a second time. An audit alert was visible (one minute).

It is clear therefore, there is both a public sector and a private sector lesson to be learned from the California symposium.

- In the public sector, the lesson is – if NY had followed up on its stings, it might have found the alleged suppression fraud in the *Healthalicious* restaurant, and if it had done so then it could have demanded that Michael Grimm install an Avatar-DTI or similar system in his restaurant as a condition of continuing in business. Tax fraud would be solved.
- In the private sector, the lesson is – if the business women in NC had entered into their partnership with an agreement to install an Avatar-DTI or similar system within their POS system, then it would be easy to see where all the revenue and expenses were. Embezzlement would be solved.

In brief, this is one of the places where good business practices align very well with good public tax policy. Avatar-DTI allows a good business practice modeled on the Apple Store solution to be adopted as a tax enforcement mechanism. It is low cost and easy to implement. This is the insight offered by this author at the California Board of Equalizations *Sales Suppression & Detection Techniques Symposium*.