3-19-2012

An American Look at Zappers: A Paper for the Physikalisch-Technische Bundesanstalt, Revisionssicheres System Zur Aufzeichnung Von Kassenvorgängen Und Messinformationenthe

Richard Thompson Ainsworth

AN AMERICAN LOOK AT ZAPPERS:
A PAPER FOR THE PHYSIKALISCH-TECHNISCHE BUNDESANSTALT,
REVISIONSSICHERES SYSTEM ZUR AUFZEICHNUNG VON KASSENVORGÄNGEN UND MESSINFORMATIONENTHE

Boston University School of Law Working Paper No. 12-14
(March 19, 2012)
Revisionssicheres System zur Aufzeichnung von Kassenvorgängen und Messinformationenthe (Book)

Richard T. Ainsworth

AN AMERICAN LOOK AT ZAPPERS:
A paper for the Physikalisch-Technische Bundesanstalt,
Revisionssicheres System zur Aufzeichnung von Kassenvorgängen und Messinformationenthe

Richard T. Ainsworth

The U.S. lags behind most other countries in the pursuit of zapper software. Sales suppression catches the attention of the Internal Revenue Service (IRS) only if the manipulation seriously impacts a taxpayer's *annual* income. This is only to be expected. The federal government secures revenue primarily through an *annual* income tax. The U.S. has no broad-based transaction tax, or federal VAT.

State and local governments on the other hand impose a retail sales tax. As a result, these jurisdictions are far more concerned with accurate sales records. On average sales taxes represent one-third of state revenue.[1]

However, the state sale tax system is not uniform. The overall system is exceedingly fragmented and localized with major variances in rates, tax base, and sourcing rules. As a result, the states very much "go it alone," and when it comes to auditing firms suspected of using zappers, none of the states have the computer forensic resources needed to properly complete a zapper audit.

It is not surprising then, that there are only three reported cases of zappers in the U.S.[2] The IRS developed each of them. State and local audits *followed* the federal audit each time. Importantly, there are no reported cases of audits sequenced in reverse (where the IRS followed a state audit) and no reported cases of a state or local government initiating a zapper audit.

The common observation in the U.S. is that enforcement against technology-facilitated sales suppression has fallen through an intra-jurisdictional crack. Neither federal nor state auditors systemically target this area. But this is changing, and the change is coming from the state side.

---

[1] Across the 45 states where the retail sales tax is levied more than $226 billion was collected in 2010. The retail sales tax is second to the state individual income tax as a revenue source. Mean state reliance was 34.2%. John L. Mikesell, *The Disappearing Retail Sales Tax*, 63 STATE TAX NOTES 777 (March 5, 2012), referencing U.S. Bureau of Census, Governments Division, *State Tax Collections Summary Report* (2010).

[2] The three cases are: (1) Stew Leonard's Dairy in Danbury Connecticut. *See*: U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), *aff'd.* 67 F.3d 460 (2nd Cir. 1995) (although the tax case was settled, the details of the fraud are preserved in these federal sentencing appeals - $17 million sales skimmed over a 10 year period, with sales tax losses of $500,000 and a final determination of $1.4 million); (2) the LaShish restaurant chain in the Detroit, Michigan. *See:* Press Release, U.S. Dept of Justice, Eastern District of Michigan, *Superseding Indictment returned Against LaShish Owner* (May 30, 2007) (indicating that $20 million is cash sales were skimmed over a 5 year period); and (3) Theodore R. Kramer who installed zappers in Detroit, Michigan area strip clubs – although in this instance the tax amounts lost are not specified. *See*: U.S. Dept. of Justice, Eastern District of Michigan, *Michigan Software Salesman Pleads Guilty to Conspiracy to Defraud the Government* (November 17, 2010).

In recent years, revenue needs have *pushed* the states to look more closely at sales tax losses.[3] The states have also taken note of successful international enforcement efforts against sales suppression in VAT regimes, and these developments have *pulled* the states to consider enhancing enforcement measures against suppression frauds. Evidence that the state picture is changing can be gleaned from legislative developments and changes in audit priorities in roughly half the sales tax states.[4]

This paper has two main parts.[5] First, it summarizes the current state of sales suppression enforcement in the U.S. Secondly, it reviews the international solutions that are attracting the most U.S. attention. A conclusion indicates likely directions for U.S. enforcement.

The Great Recession – *Pushing* State Law Changes against Zappers

Georgia is the first state to take action. On May 3, 2011 Georgia enacted H.B. 415, which added code section 16-9-62 to Georgia statutes. This law made it illegal to willfully and knowingly sell, purchase, install, transfer, or possess any automated sales suppression device, zapper or phantom-ware in the state.[6] Prior to this date only the actual fraud was penalized; now the technology that facilitates the fraud is subject to enforcement measures. Before Georgia, no state penalized fraud-facilitating technology.

On March 1, 2012 Utah followed Georgia and passed a nearly identical bill, H.B. 96.[7] On March 10, 2012 West Virginia passed its version of the Georgia law, S.B. 411.[8] On March 13, 2012 Maine also passed its version, L.D. 1764.[9] As of March 15, 2012 the legislation in each of these states awaits a governor's signature.

This is just the beginning. Similar bills are pending in six additional states: New York,[10] Tennessee,[11] Michigan,[12] Florida,[13] Indiana,[14] and Oklahoma.[15]

---

[3] During the heart of the Great Recession (2009-2010) budget deficits were rising in the states. In 2009 the National Conference of State Legislatures projected budget gaps of $84 billion in just 34 states. By 2010 the gap was $143 billion. These projections set off waives of tax increases and spending cuts that were exceptionally painful. Robert Buschman & David L. Sjoquist, *Recent State Legislative Tax Changes in the Face of Recession*, 63 STATE TAX NOTES 623 (February 20, 2012).

[4] By the authors count 20 of the 45 states with a retail sales tax are engage either legislatively or through criminal investigation in the pursuit of zappers. These states have 56.8% of the U.S. population.

[5] Because of space constraints, this paper assumes the significance of pursuing zappers. It assumes that technology-facilitated sales suppression is as prevalent in the U.S. as it is elsewhere. It assumes both an active infection rate of approximately 50% in the restaurant industry, and an overall tax system vulnerability rate of 70% for all point of sale (POS) systems in a state. But, as a powerpoint presentation by the California Investigations Division puts it:

> Does California have a problem? We most likely haven't found it yet.

Zappers and Phantom-ware: Automated Sales Suppression (March 2012) at 6 (on file with author).

[6] GA. CODE ANN. §16-9-62(b).

[7] H.B. 96, 2012 Gen. Sess. (UTAH 2012)

[8] S.B. 411, 80th Leg., Second Reg. Sess. (W. VA. 2012)

[9] L.D. 1764, 125th Me. Leg., Second Reg. Sess. (ME. 2012)

[10] S.B. 2852 & S.B. 2611 (requiring a study), 2011 Leg. Sess. (N.Y. 2011).

[11] H.B. 2226, 107th Gen. Assem., (TENN. 2011).

The Oklahoma legislation is particularly Draconian. Where each of the other states impose a penalty of up to $100,000 and one to five years in jail, Oklahoma adds a $10,000 administrative penalty and allows the Commissioner to remove the business license from the offending establishment for up to ten years if a zapper is found. Oklahoma H.B. 2576 states:

> 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.

New York and Maine have amnesties provisions for merchants who step forward and voluntarily disclose a zapper. Oklahoma and the seven other states simply penalize - immediately, and without hesitation if a zapper is found.

Aside from these legislative efforts, the author is aware of nine more states where anti-zapper laws are under active consideration, or where the pursuit of zappers has become a criminal investigation priority of the department of revenue.

Finally, among the most compelling factors *pushing* the states into action is a report that New York has conducted four successful sting operations for zappers. According to the New York Post the Department of Taxation and Finances found that when they opened up false restaurants and solicited tenders for new electronic cash registers that "most"[16] of the twenty-four ECR/POS system sales representatives who showed up actively solicited orders for sales suppression software associated with their machines.[17] The ability to digitally skim sales was clearly considered a competitive selling point.

International Solutions – *Pulling* States to Secure POS Systems Against Zappers

State and local governments are in a position to benefit from international efforts to find a solution to zappers, and they know it. On the technology side, solutions range

---

[12] S.B. 768 & 769, 2011 Leg., 96th Sess. (MICH. 2011).
[13] S.B. 1304, 2012 Leg., Sess. at §6 (FLA. 2012).
[14] H.B. 1337, 117th Gen. Assem., Second Reg. Sess. (IND. 2012).
[15] H.B. 2576, 2012 Reg. Sess. (OKLA. 2012).
[16] In other venues the Department of Taxation and Finances confirmed the NY Post report and indicated that by the expression "most" the Department meant that approximately 70% to 80% of the salesmen were offering zappers.
[17] John Crudele, *Today's Special: Scam Dodges $400M in Sales Tax*, NEW YORK POST (January 24, 2011).

from very cost-effective measures, like the INSIKA-developed smart card (€50),[18] to Quebec's far more expensive *module d'enregistrement des ventes* MEV (costing between C$600 and C$800).[19] Blended applications, like BMC Inc.'s Sales Data Controller – Mobile (SDC-Mob),[20] offer the best attributes of both of these solutions, and a bit more (US$350).[21] These technology solutions encrypt data and prevent it from being "zapped away."

Non-technology (regulatory) solutions approach the same problem differently. The Netherlands and Norway establish the government's right to control POS system data, and then marshal market forces to preserve it. The assumption in these jurisdictions is that data security can be made into a competitive factor among cash register system providers. Costs in this case are indirect and more difficult to measure.

As state and local governments measure the revenue that is being lost to zappers, these promises of technological and regulatory solutions *pull* enforcement efforts forward.

Technology-based solutions. The INSIKA smart card has caught U.S. attention. It is hard to argue with a €50 solution that offers a high degree of security for ECR/POS system transactions.[22] The smart card achieves economies by taking advantage of native ECR/POS system capacities.[23] For example, sales data is stored in the electronic journal

---

[18] Personal e-mail communication, Dr. Norbert Zisky, Head of INSIKA research (February 19, 2008) (on file with author).

[19] At a conference in Montreal sponsored by Revenue Quebec, *The First Conference on Tax Compliance – The Fight Against Tax Evasion* (June 2-4, 2010) the position of Revenue Quebec was that the MEV (also called in English translation a Sales Recording Module, or SRM) would cost C$600. On January 26, 2011, Allagma Technologies, an SRM dealer in Quebec posted the following FAQ:

> **Q: How much does an SRM (MEV) cost?**
>
> **A:** The cost of an SRM (MEV) unit is approximately **$800 plus installation fees**.

available at: http://www.allagma.com/products/srmmev-law-in-quebec/frequently-asked-questions-faq/. The difference in these numbers may have been that the conference announcement did not include the cost of a Microsoft software license.

[20] Sales Data Controller (SDC) is a generic term that applies to a lot of devices in the market that perform a similar function. They can be stand-alone or integrated into cash register systems. *See*: http://www.salesdatacontroller.com/index.php/all-about-sales-data-controller. SDC-Mob is a specific device made by BMC Inc. It is an SDC that includes secure mobile communications functionality.

[21] Tetsuo Yamada, CEO of BMC, indicated that US$350 was the price of a single SDC-Mob (November 16, 2011).

[22] The price of the smart card is critical to some people in the states. Thus, a further e-mail conversation with Dr. Zisky (March 15, 2012) was initiated to confirm this price point. He states:

> In my opinion the costs per card in a package of 10,000 pieces is $5 to 7 including all software packages, license fees and testing/certification fees. The technical solution for handling this card (readers, drivers, software development) takes … not more than $20. Based on that we doubled the costs and came to ($ or €) 50. This value is confirmed by our partners from industry.

[23] This, of course, imposes demands on the ECR/POS system, and there may be an upgrade to older business systems required in a jurisdiction that selects the smart card solution.

(EJ) not the smart card, but it is "signed" before storage. The smart card holds sums and counters, not large amounts of basic data.[24]

Even the data's signature is not stored on the card. Auditors find the signature in the EJ, import it into audit software, and then verify authenticity. Thus, the smart card's economy is also (in part) its chief liability. Un-encrypted data is stored on an open EJ. This is a potential security risk, because the EJ can be tampered with. If it is, then the auditor can detect it, but an audit must be performed to find the tampering.

Quebec's MEV solves the smart card's security problem by storing encrypted data in a tamper-proof external device. The MEV keeps a real-time clock independent of the ECR/POS system, and provides auditors with a scan-able bar code on each receipt to verify security.[25] The MEV makes system demands on a merchant's cash register. In some instances a new cash register is needed, and this can be a considerable expense for small businesses.[26] Although the MEV has additional functionality,[27] it is questionable whether or not its price at fifteen times the cost of an INSIKA smart card returns fifteen times the security.

BMC's SDC-Mob provides a third-party solution that matches the capabilities of the government-involved solutions (INSIKA smart cards and the MEV) at half the price of an MEV. Transaction data is encrypted. It is signed with an INSIKA-like smart card.[28] Data is securely stored externally. SDC-Mob data can also be accessed remotely to assure compliance, and a check for tampering can be made without leaving the tax office. This kind of system appears to be acceptable under the new Belgian regulations, however if adopted, the smart card will not be INSIKA's (rather a Belgian card

---

[24] A companion issue concerns the real-time clock, which originates with the ECR/POS system, not the smart card. The smart card includes output from the real-time clock in its encryption algorithm, but to the extent a fraudster would want to tamper with the clock he would have access to it in the insecure ECR/POS system. Changing the clock might be a technique used to confuse an auditor.

[25] *See*: Revenue Quebec, *Fight Against Tax Evasion: Sales Recording Module (SRM)* (describing the SRM system) *available at*: http://www.revenuquebec.ca/en/a-propos/evasion_fiscale/restauration/mev/.

[26] Ministry of Revenue Quebec, *Fight Against Tax Evasion: Point-of-Sale (POS) Systems*, indicates:

> As a restaurateur, you are responsible for ensuring that your POS system is SRM [MEV] compatible and that it can communicate with an SRM [MEV]. To be SRM [MEV] compatible, your POS system must be adapted by its developer to meet our requirements and technical specifications. Developers can request that an adapted POS system be certified compliant with our technical specifications. If the adapted POS system is compliant, we issue a confirmation of certification that recognizes the compatibility of the product with an SRM [MEV]. [This page list 81 compatible systems.]

Available at: http://www.revenuquebec.ca/en/a-propos/evasion_fiscale/restauration/produits.aspx. That this may pose a considerable hardship for some merchants is explained in Anja Karadegllja, *Deadline Looms for Restaurant Rebates,* ACTUALITES (February 17, 2011) (which considers how a $2,000 ECR upgrade in one business and a $6,000 upgrade in another to accommodate the MEV placed these businesses in considerable financial difficulty, even though Quebec was providing subsidies for merchants), *available at*: http://www.lesactualites.ca/?site=CDN&section=page&1=C110216&2=C110119_deadline.

[27] The MEV is manufactured by AAEON, a Taiwanese company. The full commercial version with technical specifications can be seen here: http://www.aaeonsystems.com/products/AEC-6831.php.

[28] The SDC-Mob could use the INSIKA smart card, or as in Belgium a different smart card could be developed locally and used in the device.

developed by Fedict[29] would be required), and the mobile attribute will be eliminated on political/privacy grounds.[30] This approach is similar to the Swedish solution.

From a U.S. perspective, the implementation methodologies of some of these international solutions create difficulties. The MEV is required in *all* Quebec restaurants, and the earlier version of the SDC-Mob (the eTax module)[31] is certified for use in a program that mandates it in *all* Swedish cash registers. In the U.S. a similar *technology mandate* would represent a deep government-intrusion into business privacy/ confidentiality. Proof of a compelling state reason to do so might be needed.[32]

The German use of INSIKA smart cards in taximeters is a different story. There is a considerable problem with skimming cash sales by German taxicab operators. Both the taxicab owners and the revenue authorities are loosing revenue. However, without *requiring* smart cards in *all* taximeters, the city of Hamburg established a *voluntary* program with a grant of €5 million for the adoption of taximeters that would be secure against data manipulation.[33] The Hale taximeter company has installed the INSIKA

---

[29] Fedict is a Federal Public Service of Belgium, created on May 11, 2001 as part of the plans to modernize the federal administration. It is a so-called horizontal Federal Public Service because it isn't responsible for a specific policy field, but provides services to the other Federal Public Services. Fedict is responsible for e-Government. *See*: http://www.fedict.belgium.be/en/

[30] As of March 16th, 2012, the Belgian regulations have not been finalized, however they have been reasonably well developed for some time. They were expected to have been finalized by the end of 2011. They are the topic of inter-governmental studies, and are considered for example in the Norwegian study *New Regulations for Cash Register Systems* (*Nytt regelverk for kassasystemer*) at 37-39 (in Norwegian, translation of file with author). They also play a significant role in a Dutch Master's thesis by M. Leurink, *Beheersmaatregelen ter Voorkoming en Bestrijding van Datamaipulatie in Afrekensystemen* (Management Measures to Prevent and Combat Data Manipulation in Cash) (March 2011) at 36-44 (in Dutch, translation on file with author) *available at*: http://www.keurmerkafrekensystemen.nl/wp-content/uploads/2011/05/Beheersmaatregelen_tav_datamanipulatie_afrekensystemen_Leurink_mrt2011.pdf.

[31] Swedish certification (by SWEDAC) was awarded to an earlier version of the SDC-Mob called eTax on August 24, 2009. Post-2009 development efforts by BMC included working with a smart card (like the INSIKA card) and the inclusion of remote communications (the Mobile attribute in the SDC-Mob). What is important in this regard is to notice the responsiveness of the private sector to developments in the security field. By positioning itself as a standard-setter the Belgian government is pushing the private sector to adopt and adapt to cutting-edge solutions.

[32] *See*: Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Georgetown Law Journal 123 (2007) (suggesting that the American law of privacy and "inviolate personality" differ from the English concept of confidentiality which recognizes and enforces expectations of trust within relationships, and in this case the concern might be with confidentiality). Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO LAW REVIEW 745 (2007) (arguing that there is a threat to privacy in data mining and other oversight activities even when the government does not uncover illegal activities).

[33] The voluntary Hamburg program can be seen at: http://www.hamburg.de/taxi/3030326/taxameter-foerderung.html. The Hamburg grant is for €1,500 euro per participating taxi.

smart card and currently offers the only solution on the market.[34] The program is reportedly a success.[35]

The four New York stings operations that found a high incidence of ECR/POS system salesmen also selling zappers is a start down the *mandatory* road, but these stings do not compare with the 230 litigated cases of restaurants using zappers in Quebec. Quebec was able to impose the MEV on all restaurants in the province because it had proof of widespread fraud.[36] That is not the case in the U.S., and the states may need to be looking at a program similar to the German's voluntary taximeter program.

Non-technology (regulatory) solutions. Jurisdictions that *regulate* solutions to zappers have a different focus, and a different proof-point than those that apply technology – their focus is the ECR/POS system, not the businesses that use them. The difference is subtle, but the problem is the same. Stated another way:

- A *regulatory solution* needs to prove that the *cash registers* in the commercial marketplace are inherently vulnerable to manipulation. It then regulates equipment improvements so that the systems will never manipulate transactions.
- A *technology solution* needs to prove that *businesses* are exploiting cash register vulnerabilities. It then monitors use of the equipment in a way that records manipulations whenever they occur.

Thus, the goal of regulation is to get manufacturers to produce *only* secure machines. In this regard, the Dutch and Norwegian approaches to zappers are good examples of how the regulatory approach works. There are differences in application.

The Dutch *persuade* manufacturers to improve security; the Norwegians *specify and demand* the improvements they want. The underlying premise is the same – there is a marketplace problem. The premise has a corollary: manufacturers will ultimately provide the best oversight when (*and only when*) commercial rewards align with data security.

Netherlands. Following the discovery of a zapper developer at a manufacturer of POS systems (2010) the Dutch Tax Administration (*Belastingdienst*) took the client list and asked each purchaser of this POS system to sign a statement that declared:

- The type of cash register used
- Whether they used the installed zapper

---

[34] The Hale taximeter system with INSIKA smart card can be seen at: http://www.hale.at/en/solutions/fiscal-solutions/insika-solution.html.

[35] In the 2010-2011 time frame the PTB conducted a voluntary pilot program (up to 10 taxis in Hamburg and another 10 in Berlin). Within the past six months Dr. Zisky reports that the pilot has recorded 13,000 trips without an error. (Personal e-mail from Dr. Zisky on March 16, 2012, on file with author).

[36] Roy Furchgott, *With Software, Till Tampering Is Hard To Find*, NYT C6 (August 20, 2008) (indicating that Revenue Quebec had brought 230 zapper cases to court in ten years) *available at*: http://www.nytimes.com/2008/08/30/technology/30zapper.html?scp=1&sq=With%20Software,%20Till%20Tampering%20Is%20Hard%20to%20Find%20%20comments&st=cse

- Whether they were willing to repay lost tax revenue (if any)[37]
- Whether they were willing to take steps to prevent future fiscal damage.

Following up on the related enforcement action the public (with considerable assistance from the press where this was a big news story) became convinced that the *Belastingdiest* could find any non-compliant cash register. Based on these reports, and the signed statements, which included a promise to prevent future frauds, there very quickly was a noticeable increase in demand for complaint machines. For this purpose (and to help the industry meet this need) the *Belastingdiest* met with over 70 producers and traders of cash registers. An agreement was reached among all parties (including a signed letter of intent on April 18, 2011) that resulted in:

- A set of standards for reliable cash registers;[38]
- A Quality Mark (*Het Betrouwbare Afrekensysteem*) that would indicate that a cash register met compliance standards; and
- A commitment by the producers and traders that after July 1, 2013:
    - No POS system would be sold that could not achieve a Quality Mark;
    - All simple cash registers would have a declaration of settings by the producer.[39]

If the Dutch are successful in their cooperative-regulatory approach to zappers, there will soon be no possibility for technology-assisted sales suppression fraud in the Netherlands. After July 1, 2013 no cash register system sold in the Netherlands will be vulnerable to a zapper.

Norway. On February 15, 2012 the Norwegian Ministry of Finance released the Directorate of Taxation's report, *New Regulations for Cash Register Systems* (*Nytt regelverk for kassasystemer*),[40] and placed it into public consultation until May 15, 2012.

The report essentially recommends that only qualifying cash register systems be allowed in Norway. Suppliers of cash registers will be required to upgrade current systems, and make initial and ongoing product declarations to the tax office that the functional requirements of the regulations are met by their systems. Operators will be required to acquire new or upgrade current systems and then notify the tax administration of the change.

> Secure electronic records should therefore be Norway's answer to the hardware-based security used in foreign countries through control boxes, smart cards, etc.[41]

---

[37] "About 85% did not use the zapper module, 15% however did." Ben G.A.M. van der Zwet, (*Belastindiest* computer forensic auditor) *A Pebble in the Cash-Economy* (draft, on file with author)

[38] The standards are produced by an independent Quality Mark authority, *Stichting Betrouwbare Afrekensystemen* (Reliable Cash Register Foundation) which can be found at: http://www.keurmerkafrekensystemen.nl/. Essentially, those standards are classified according to four management objectives: (1) register all events; (2) integrity of registrations; (3) storage of registrations; and reports are transparent and reliable.

[39] The declaration of settings is specific to each type of simple cash register, but it will describe all system attributes (no hidden capacities that are not described are allowed). It will lead to a Quality Mark.

[40] *Available at*: http://www.regjeringen.no/pages/36992076/h_notat_10_4626_HS.pdf (in Norwegian)

The revenue gain is projected to be substantial.[42]

The Norwegian view is that product declarations, notifications and fines "… act as a substitute for a technical solution."[43] The Cash System Act (*Kassasystemloven*) sets out the requirements of checkout systems (§3), a duty for suppliers of checkout systems to assist the tax office with software, programming, and operation of their systems (§4), requirements for product declarations by suppliers (§5), a set of seven violation fees imposed on suppliers (§6), and daily "coercive fines" also imposed on suppliers (§7). In addition, regulations are authorized (§8).[44]

The cash register system regulations (*Kassasystemforskriften*) are extensive. Most notable are the regulations at §2-5 that specify the features that a cash register must have, and those at §2-6 that specify prohibited features.[45] Cash registers that violate these rules must be "pulled from the market, unless the supplier rectifies the deficiencies."[46] Enforcing this provision is expected to be relatively easy as the supplier and user will register each cash system (by government issued ID) in an online database.[47]

Fourteen additional fines and fees are specified in the Bookkeeping Regulations (*Bokforingsforskriften*) that deal with the operator's use of the cash register system.[48]

The U.S. Way Forward

It is certain that the U.S. states are listening and learning from the experiences of the international community in the battle against technology-assisted sales suppression. At the moment at least nineteen states are engaged in some form of legislative or administrative enforcement actions today.

Admittedly, there is very little to show for this effort if we are using litigation as our yardstick. As of March 15, 2012 there is no public evidence that any state has initiated an audit on a firm that has used a zapper or phantom-ware to skim sales. All state cases are those where the state is following a federal income tax audit.

However, we may well be on the cusp of change in the U.S. Preparations for enforcement action are underway. Laws that penalize the sale, purchase, installation,

---

[41] *Id.*, at 60.
[42] An independent IT consulting firm indicated that adoption of these rules would provide an estimate net present value gain of 14.092 billion NOK or $2.48 billion USD over ten years. Steria AS, *Skattedirektoratet: Prosjekt "Nytt regelverk for kassasystemer" – Samfunnsokonomisk analyse* (Tax Directorate: Project "New regulations for checkout systems" - Social Economic Analysis) (September 21, 2011) at 28, Table 5, *available at*: http://www.regjeringen.no/pages/36992076/vedlegg_steria.pdf (in Norwegian).
[43] *Nytt regelverk for kassasystemer*, *supra* note 40, at 62.
[44] *Id*., 97-98.
[45] *Id*., at 99-100.
[46] *Id*., at 63.
[47] *Id*., at 63.
[48] *Id*., at 67 & 104.

transfer, or possession of any automated sales suppression device, zapper or phantom-ware have been enacted in one state (Georgia) and passed by the legislature in three others (Utah, West Virginia and Maine). Four highly productive stings have been conducted in New York.

Next steps in the U.S. This is the most interesting compliance question. What enforcement direction will the states move in, as suppression frauds are uncovered? Will a technology solution like the INSIKA smart card, the Quebec MEV or BMC's SDC-Mob be the route, or will a regulatory approach be used? If the later, will the states try to *persuade* cash register providers to comply with industry formulated rules like the Dutch, or will they *mandate* that providers make changes (and the users adhere to them) like the Norwegians?

Will any of these solutions work in the U.S. if they are applied universally throughout a jurisdiction (as in Sweden, or Norway), or throughout a discrete business sector, like the restaurant sector (as in Quebec and Belgium)?

A privacy push-back. The most interesting legal question deals with privacy. How will state tax administrations respond to a "business privacy" push-back?

Privacy concerns may move enforcement into more surgical responses than we have seen internationally (outside of the German use of the INSIKA smart card in taximeters). States may adopt the adage that "every dog deserves one bite," and give the Commissioner authority to mandate one of the international solutions case-by-case, and only in certain defined situations. Perhaps the rule would isolate businesses that have been shown to be regularly out of compliance with the sales tax, or with historically bad records, or with especially contentious audit positions. Maybe the rule would be even narrower and apply only to businesses that have been found to be using a zapper or phantom-ware applications.

In these instances a businesses might be required by the Commissioner to install a technology solution like the SDC-Mob, which can be remotely overseen by tax authorities. Or perhaps a Norwegian approach might be authorized, and regulations could be drafted that would force problematical businesses to install cash register systems that are manufactured with security features like those required in Norway. Such an approach would be more lenient than simply revoking the sales tax permit, as Oklahoma is prepared to do.

Not Just Cash – Debit/Credit Transaction Too

One final point needs to be made. Technology-assisted sales suppression is no longer just about *cash* skimming; this fraud has migrated to *debit/credit card* transactions. There are two indications that this is happening, and that zappers are key instruments in facilitating it, one from Norway, and the other from the recent Fiscalis meeting in Ireland.

Norway. The recent Norwegian regulatory proposals include a discussion of "problems related to the terminal – use of an independent terminal." In short the problem involves debit/credit card terminals that are not connected to the cash register system. If the terminal is programmed to remit funds to a different (personal) account at a different bank (not the bank used by the business making the sale), then a sale can be rung up "as if" it was a cash sale and then zapped as follows:

1. The cashier scans the purchase;
2. The cash register indicates a sales total ($500, for example);
3. The credit/debit card is swiped for $500;
4. An authorization is received from the debit/credit card intermediary;
5. The cashier then presses "cash sale," (not credit/debit card sale) a receipt is issued, and the transaction completed;
6. Later that evening the false cash sale is "zapped" from the system.

Neither the debit/credit card transaction (at 3 & 4), nor the sales transaction (at 6) is recorded in the cash register system. There is no digital trace for a traditional auditor to follow to determine liability, unless the auditor knows the credit/debit card that was used, and traces the payment from the cardholder's bank to the (personal) account of the business owner.

The Norwegian regulations solve this problem by requiring debit/credit card terminals to be tied to the cash register.[49]

Irish Fiscalis meeting. How significant is this permutation of sales suppression? Significant enough so that nearly a full day of meetings at the E.U. Fiscalis held in Dublin, Ireland (October 19-21, 2011) were devoted to this problem with reports filed on the problem by the UK[50] and Portugal,[51] followed by workshops focused on combating this fraud.

The U.S. states need to take this permutation of sales suppression fraud into account as they devise their way forward. The international community is already doing so. This mutation appears to be significant.

[49] Checkout System Regulations (*Kassasystemforskriften*) § 2-5, second paragraph; § 2-8-3 and § 2-8-2(g); Bookkeeping Regulations (*Bokforingsforskriften*) § 5a-2, second paragraph; § 5a-14, third paragraph.
[50] Chas Coysh, HMRC Indirect Tax Team, Strategic Risk Unit, Large Business Services. His Friday, October 21, 2011 presentation focused on Merchant Acquirer Accounts – Tax Evasion in the U.K.
[51] Ana Isabel Silva Mascarenhas, the e-Audit Contact Person for the Portuguese Tax Administration, who presented on fraud with Merchant Acquirer Accounts in Portugal.