ZAPPERS – SKIMMING CASH WITH TECHNOLOGY

Richard T. Ainsworth

Skimming cash receipts is an old-fashioned tax fraud; a fraud traditionally associated with small- or medium-sized enterprises. Large businesses with formalized internal control mechanisms, external accountants, and professional management structures do not normally engage in skimming. Businesses that skim frequently keep two sets of books (one for the tax man, the other for the owner). In its simplest form there are two tills, and the cashier simply diverts some cash from selected sales into a secret drawer. A record of the diversion may be maintained, but it will be kept outside the formal accounting system. Businesses that skim rarely do so with credit card transactions precisely because these sales can be documented externally through the banking system. Skimming frauds thrive when the owner (or a close family member) is the cashier.

Technology is changing how businesses skim. The agents of change are software applications – Phantom-ware and Zappers.[1] Phantom-ware is a "hidden," pre-installed programming option(s) embedded within the operating system of a modern electronic cash register (ECR). It can be used to create a virtual second till and may preserve a digital (off-line) record of the skimming (a second set of digital books). The physical diversion of funds into a second drawer is no longer required, and the need for manual recordkeeping of the skim is eliminated. Because Phantom-ware programming is part of the operating system of an ECR, its use can be detected with the assistance of a computer audit specialist.

Zappers are more advanced technology than Phantom-ware. Zappers are special programming options added to ECRs or point of sale (POS) networks. They are carried on memory sticks, removable CDs, or can be accessed through an Internet link. Because Zappers are not integrated into operating systems their use is more difficult to detect. Zappers liberate owners from the need to personally operate the cash register. Remote skimming of cash transactions is now possible without the knowing participation of the cashier who physically rings up the sale. This attribute of Zappers allows the incidence of skimming fraud to migrate beyond the traditional "mom and pop" stores. Zappers allow owners to place employees at the cash register, check their performance (monitor employee theft), but then remotely skim sales to cheat the taxman.

It is something of an anomaly that Zappers and Phantom-ware appear to be a very serious problem in wide range of developed countries (Canada, the Netherlands, Germany, Brazil, Australia, and Sweden), but they do not appear to be a concern in the United States. In fact, there are only two Zapper cases in the United States, the $17 million skimming fraud at Stew Leonard's Dairy (a grocery store) in Connecticut[2] and the $20 million skimming operation at the LaShish restaurant chain in Michigan (U.S. Department of Justice, 2007a). It is alleged that the cash skimmed at the LaShish was used to finance Hezbollah terrorists in Lebanon (U.S. Department of Justice, 2007b).

CAN THE UNITED STATES LEARN FROM QUEBEC?

The American experience with Zappers contrasts dramatically with the Zapper enforcement activity of the Quebec Ministry of Revenue (MRQ). If over 230 Zapper cases have been prosecuted over the past 10 years just across the border, is there something America can learn from the MRQ?[3]

The MRQ first discovered that Zappers were in wide use in 1997, and has engaged in an aggressive enforcement action ever since. Some of the highlights of this activity over the past 10 years include, for example, the Audio Lab investigation, the Stratos restaurants' investigation, and the investigations related to Mr. Luc Primeau.

The Audio Lab investigation first became public on April 8, 2004 after search warrants were executed at the San Antonio Grill, a restaurant in Laval, Quebec. The allegation was that a "sales Zapper" (*camoufleur de ventes*) was used to delete sales records (Revenue Quebec, 2004). The owner pleaded guilty one year later.[4] But, more importantly, on October 14, 2005, Revenue Quebec announced that it was executing five more search warrants in Montreal and Laval on Audio Lab LP, Inc. as it was under suspicion of having developed and marketed the sales Zapper used in the cash registers at San Antonio's Grill. Audio Lab LP, it turns out, not only developed the operating software in the cash registers at San Antonio's Grill (called Softdine),[5] but it developed and sold the Zapper that defeated it.

On June 26, 2007 Audio Lab LP, Inc. pleaded guilty to charges of having, "… designed and marketed a computer program designed to alter, amend, delete, cancel or otherwise alter accounting data in sales records kept by means of a software that [Audio Lab LP] had designed and marketed." (Revenue Quebec, 2007)

The Stratos restaurants' investigation highlights two other characteristics of large scale technology-assisted skimming frauds: the way the cash generated by the fraud is used to corrupt people doing business with the "zapping" enterprise, and the ease with which this fraud can sweep through a chain of related businesses. To dispose of the excess cash from skimmed sales (1) a double-billing system was put in place with suppliers (to conceal purchases made in cash), and (2) wages were paid to employees in cash (without being reported as income). All together 28 Stratos restaurants became involved. Guilty pleas came in waves – 19 companies pleading guilty on September 26, 2002; another 6 pleading guilty on October 11, 2002, and the 4 remaining pleading guilty on March 21, 2003.

Press releases provide details of only the final 10 companies. In aggregate the taxes and penalties for these companies came to $1,816,070.90, but the real thrust of the news releases were that "… the Department has conducted searches in order to establish proof that the designer of the IT function associated with the cash register software Terminal Resto had participated in the scheme set up by restaurants in the Stratos chain."[6] On April 25, 2003, Mr. Michel Roy and his two sons, Danny and Miguel, admitted that they were guilty of facilitating the Stratos tax evasion. The father (Michel) was the creator of the Zapper that worked with Resto Terminal. He promoted it and made the sales. His sons (Miguel and Danny) were also implicated in creating the Zapper. Aggregate fraud penalties assessed against the Roys were $1,064,459 (Revenue Quebec, 2003c).

The third example involves Mr. Luc Primeau, a software designer who became the focus of an investigation that began with the announcement on March 17, 2003 that seven Patio Vidal restaurant franchises and a bar, La Tasca, from Gatineau, Quebec, as well as another bar named O'Max in Masson-Angers, Quebec were convicted of adding Zappers to their Microflash cash register software (later upgraded to a new version called Caracara). Mr. Primeau not only designed Microflash and Caracara, but was the developer of the associated Zapper program that these businesses used (Revenue Quebec, 2003a).

On October 17, 2005 Mr. Primeau admitted that his software assisted these companies to evade $435,000 in GST and QST. All together these companies skimmed $2.7 million in cash sales. Mr. Primeau was fined for his involvement, but more importantly for this analysis, Mr. Primeau represents the software designer who becomes a real threat to the tax system by morphing into a business consultant. Mr. Primeau actively spread Zappers and brought this fraud to a series of bars and restaurants.[7]

MEASURING SIGNIFICANCE

How serious of a revenue problem is sales suppression (as a general matter)? Has it been/ can it be measured? Two governments have reportedly conducted studies of automated sales suppression – Quebec and Germany. In both cases the studies supported proposals for legislative change. Neither government has made the full studies available, although summaries of their conclusions have been released. These studies reach similar conclusions.

Quebec

The government of Quebec has conducted two studies of automated sales suppression. The Quebec studies also focus on the restaurant sector. The first study followed the customer list of an early Zapper distributor/developer.[8] This investigation (the First Inspection Wave) examined 70 systems and uncovered 41 Zappers.[9] This was followed by a more statistically accurate investigation (the Second Inspection Wave) that was based more broadly on a random sampling of businesses within the restaurant and hospitality industry. This survey, conducted by Finances Quebec, found that 16 percent of all sales went unreported.[10]

Both of these studies where relied upon by the Quebec Minister of Revenue, Jean-Marc Fournier, when he announced legislative changes, enhanced enforcement efforts, and a pilot project designed to counter the penetration of sales suppression technology in the restaurant sector on January 28, 2008. He indicated:

> Although the majority of restaurant owners comply with their tax obligations, the restaurant sector remains an area of the Quebec economy where tax evasion is rampant, both in terms of income taxes and sales taxes. Tax losses in this sector are significant. Revenue Quebec estimates them at $ 425 million for the 2007-2008 fiscal year.[11]

Germany

The Interim Report of the German Working Group on Cash Registers indicates that the Group was "… aware of [technology-assisted] fraud amounting to 50% of companies cash receipts."[12] The Working Group does not separately quantify the kinds of *technology-assisted* fraud involved; in other words it does not consider whether Germany has a Phantom-ware or a Zapper problem. Most likely, Germany is experiencing both (and more).

The Working Group's 50 percent observation is supported by a report made by the German Federal Audit Office (BHR) to the German Parliament in 2003. In this report the BHR appears to focus only on factory installed software (self-help Phantom-ware).[13] The BHR concludes that the potential loss in Germany is in the billions of euros:

> The Federal Audit Office (BHR) has complained that later models of electronic cash registers and cash management systems now fail to meet the principles of correct accounting practice when it comes to recording transactions … The risk of tax fraud running into *many billions* [of euro] should not be underestimated in cash transactions.[14]

Both the BHR's observations and the Working Group's study are further buttressed by summaries from studies conducted by three German federal states. These studies are limited, because they focus only on the restaurant sector. But, they too conclude that sales suppression is a significant problem:

> One federal state is currently implementing a special "restaurant" initiative. Checks already made have led to average upward revisions of 46% of original turnover. A comparable initiative in another federal state resulted in over half the cases (54%) having upward revisions of 60% of declared turnover. Fraud amounting to 25% was detected in a fifth of the cases, and was as high as 5% in the remaining 26% of cases. A third federal state has found that around 45% of till receipts involving cash are subject to upward revisions ranging from 20% to 118%.[15]

SOLVING THE PROBLEM

Since the presentation of this paper at the NTA conference I have received a number of e-mails from a woman in New York City whose divorce is not going the way she thought it should (financially). It seems the four restaurants she owns with her estranged husband are suddenly not showing profits. In fact there are losses. Cash infusions are needed to keep the businesses running.

Her accountant has been over the books repeatedly. The cash register records check out and tie to the financial reports, the bank deposits confirm that cash receipts are deposited, and even though spoilage is a little high nothing seems amiss in the numbers. What bothers her most is that the businesses are running at normal customer volumes. Employee levels (chefs, waiters, bar tenders) are stable, inventory purchases are normal, only the gross sales and profits are down. Her husband is the head chef in one of the restaurants.

There was a new POS (point of sale) system which her husband had convinced her that the restaurants needed. The POS was integrated into the ECRs (electronic cash registers). But, as long as each customer's receipt was being rung up (and she is convinced that they are), then she cannot understand why her accountant cannot not find the money she assumes is missing. She has heard about Zappers "on the street," and now suspects that along with the new POS system a Zapper may have been installed in the restaurants. This is not something she expects her accountant to find, so she has been asking for technology referrals.

The point of this story is *not* that Zappers are being used in New York to suppress sales data. I think we all assume that Zappers are here (even though there is limited federal, state, and local tax audits uncovering them). Instead, the point of this story is that Zappers work in a commercial marketplace, and the players in this market have competing interests. At different times different players will be insisting on accurate records; and, when they do, their interests will align with those of the tax administration.

In such an environment governments that certify the accuracy of ECRs and POS systems have low cost, well informed, and highly motivated allies in the tax enforcement effort. The key is for governments to realize that they have the authority to not only evaluate compliance after the fact (traditional audits), but they can regulate the contemporaneous marketplace in a manner that will require the market to self-verify cash records for all the players (certification).

Take for example the case of a Wendy's Restaurant franchise in Illinois. In this case the Illinois Department of Revenue (sales tax) and the IRS (income tax) were on Wendy's side opposing a bankruptcy petition by Noah and John Robinson. The Robinsons were the franchise holders for six Wendy's restaurants outside of Chicago. By skimming cash sales at their franchise locations, the Robinsons not only engaged in sales and income tax fraud, but they defrauded Wendy's International of franchise and advertising fees that were based on a fixed percentage of gross sales.[16] If sales were required by state law to be rung through certified cash registers in Illinois, it would have been a simple matter for Wendy's, the State and the IRS to find the skimming.

SECURING THE FISCAL TILL

Aside from simply enhancing traditional audits with a cadre of computer audit specialists there are a range of technology intensive solutions to Zappers and Phantom-ware that governments can use. This article considers the Greece, Quebec, and Germany approaches to securing fiscal tills in real time.

GREECE

Greece has had comprehensive fiscal till legislation in place for over twenty years. Considered as a whole, the Greek approach is to secure data both at the time when orders are first entered into an ECR, and when the ECR's printer is issuing the final receipt.

Under Greek rules all tax-related documents are required to be digitally signed. All Greek businesses, whether they use ordinary stand-alone cash registers or cash registers equipped with advanced connection capabilities (network or PC-operated machines), must use certified machines.

Data from the electronic memory is signed by a secure hash algorithm (SHA-1).[17] This hash value is permanently safeguarded and stored in the fiscal memory. Daily sums (total sales receipts and tax amounts) are saved into the fiscal memory, cumulatively and on an itemized receipt basis. This function essentially preserves the X and the Z Reports along with the Electronic Journal.

Costs vary for these machines from €200-250 to €800-1,000 depending on the manufacturer. Every manufacturer, developer, or importer of ECRs into Greece must seek approval for each specific model that they intend to sell in the Greek market. A license to sell a specific ECR is issued by a special (technical) government body. The license will issue only when the ECR conforms to all statutory technical specifications.

Once a model has successfully passed all tests, the committee issues and gives to the interested company a unique license number for the specific model. The license number is recorded by the National Wide Information Center of the Ministry of Finance and is printed on each receipt ("legal receipt") issued in each retail transaction. In addition, this number is required to be placed on a label that is visibly fixed to each machine. As a result, the certification of a specific ECR can be checked both through a visual inspection of the machine and by matching the license number on a machine with a given receipt.

Through the certification process, the Ministry of Finance preserves a copy of all approved firmware. It is a simple matter to calculate a checksum value (CRC-32[18] or SHA-1) for the object code of the firmware. Any auditor can then read the contents of the program memory of a certified ECR and determine if changes have been made in the firmware (through Phantom-ware or Zappers) by comparing his reading with that of the file kept in the Ministry of Finance.

QUEBEC – MEVS

Quebec is responding to sales suppression fraud much like Greece, but on a much more limited scale. The problem identified in Quebec is the widespread use of Zappers and Phantom-ware in the restaurant sector.

Like Greece, Quebec approaches the sales suppression problem from an adequacy of business records perspective. Quebec supplements technology solutions with very aggressive traditional audits. The business records that Quebec is primarily concerned about are the Z and X Reports, the Electronic Journal, as well as all of the digital supporting files that are kept in an ECR or POS system. These are the records that reside within an ECR and are presumed accurate because they are the basis of the data sent to the printer to produce the customer's "legal receipt."

The legal receipt is the central enforcement document in all fiscal till jurisdictions. Quebec mandates that all restaurant sales be accompanied by a receipt, and then further specifies that this receipt must pass through the *module d'enregistrement des vent* (MEV) where it is e-signed.

Penalties for not issuing a legal receipt are serious. The 2006-2007 Budget for Quebec summarized the penalties as follows:

> Restaurant operators who fail to remit an invoice to a customer will incur a penalty of $100 as a result of this omission and will commit an offence for which they will be liable to a fine of no less than $300 and no more than $5,000. For a second offence committed within five years, the fine will be no less than $1,000 and no more than $10,000, and for any subsequent offence within that period, no less than $5,000 and no more than $50,000. (Finance Quebec, 2006, pp. 144-145)

The legal receipt can be a very effective tool against collusion. If an establishment conspires with its customers to charge a lesser amount in exchange for engaging in cash transactions unaccompanied by a formal receipt, then the restaurant operator is in violation of the legal receipt rule.

Revenue Quebec's MEV pilot project is scheduled to begin in late 2009. Participating restaurants will install an MEV microcomputer between their ECR or POS system and receipt printer. The MEV will receive data from specified transactions (the drafting of guest checks, register receipts, or credit notes). From the extracted data, the MEV will produce an encrypted numerical signature, and transmit it to the printer where it will be printed on the receipt from which it was derived. Both the e-signature and the recorded data will be preserved within the fiscal memory of the MEV for seven years. Restaurants will be required to submit sales summaries, generated by the MEV, when they submit their tax declarations.

GERMANY

The German solution involves encrypting critical data from the ECR on smart cards securely embedded in ECRs. The German National Metrology Institute (PTB: Physikalisch-Technische Bundesanstalt) is the home of the INSIKA project (Integrierte Sicherheitslösung für Kassensysteme – Integrated Security Solutions for Cash Registers). INSIKA demonstrated an effective smart card on February 18, 2009 at a Berlin conference.

The essence of the German solution revolves around cryptography and smart card access to cryptographic data preserved within the cash register or POS system. If the revenue authority audits it can access the records of the cash register with a "key" to read the data and determine if there has been tampering.

The German solution is a fiscal till solution, but it is far more flexible and potentially more comprehensive that either the Greek or the Quebec solutions. The German mandate is for all ECRs and POS systems to be fitted with a smart card containing a crypto processor that e-signs designated "tax-relevant data." With this device, the entire Electronic Journal could be signed on a regular basis, or each transaction open or closed (sale, refund, training session, voided sale, or temporary record) could be designated as a tax relevant and signed whenever entered into the ECR. It would not matter under the German system if no receipt was issued. It would only matter that each item be registered in an ECR or POS system that is fitted with a smart card.

The government can conduct audits remotely. A data feed can be taken directly from ECRs. Neither the Greek nor Quebec solutions can do this. The Quebec MEV does present ECR data in a digital format, and could be used for remote audits, but this expansion of audit capability has been rejected by the MRQ on policy and privacy grounds.

One of the key features of the German solution is its low cost. The overall cost is €50 per ECR.

STREAMLINED SALES AND USE TAX (SSUTA)

Currently 19 states are certifying software systems that determine sales taxes under the SSUTA. The SSUTA could be a useful template for jurisdictions seeking to develop less intrusive and less expensive methods for combating automated sales suppression.

Currently certified service providers (CSPs) under the SSUTA perform all consumption tax compliance functions for their clients. They determine taxability and the correct rates. They prepare and file returns, make tax payments, and immunize the taxpayer from liability for errors (except taxpayer fraud).

Extending the CSP's obligations to include certification by the CSP that a taxpayer's ECRs and POS systems are free from Zappers and Phantom-ware would create a new enforcement regime. Four questions need to be addressed: (1) How does a CSP get ECR and POS system data? (2) How would a CSP know the data it has is accurate? (3) What standards should the government use to certify a CSP's automated system? (4) What is the most efficient and cost effective way for a CSP to satisfy this standard?

1. How would a CSP get ECR and POS system data?

CSPs currently pull data directly from the ECR or POS system to determine taxability. This data is stored in an independent (tamper-proof) audit file before it is used by the taxpayer to draft the invoice (receipt). The CSP maintains this file to protect itself from liability.

A "legal receipt" is not required with a CSP-based system. It could be mandated to combat fraud occurring outside the ECR, or maybe as a further tool against the consumer-business collusions, but it is not necessary for the CSP.

2. How would a CSP know that the data it has is accurate (free from manipulation)?

This is a key question. The most effective way to do this is to *adopt the German smart card* in the private sector. The German smart card can be configured to sign every event – completed sales, temporary records, refunds, test modes, open or partially completed transactions. Every key stroke can be recorded, collected, and encrypted on the smart card, and then transmitted to the CSP. Questions about any transaction, or the business records associated with any ECR, could then be directed to the CSP. Only in cases of fraud would it be necessary for the tax administration to approach the taxpayer. If suspicions were raised, it would be in the self-interest of the CSP to assist the government in determining the truth.

This would be a form of comprehensive ECR monitoring, but it is the private sector monitoring the private sector, not an intrusive government oversight program.

3. What standards should the government use to certify a CSP's automated system?

The data preservation standards that a CSP would need to meet if it were to certify the accuracy of business records in an ECR should be the same standards that a principles-based jurisdiction, like the Dutch, would set down for all ECRs. In *Your Cash Register and the Fiscal Accounting Obligations*, the Dutch Tax Authority lists the requirements for a business wishing to bring their ECRs or POS system into compliance with Dutch law. They include:

- Detailed records available for the tax auditor if and when required
- Electronic preservation of the details of transactions
- Preservation of a complete audit trail
- Taking adequate measures to guard against subsequent alterations in a manner that will assure that data-integrity is maintained.

Under the SSUTA model, a service provider could not be certified unless it could assure tax authorities that its system accurately, completely, and automatically captured this data from the taxpayer's ECRs. With this data on hand the CSPs attestations would be highly credible.

4. What is the most efficient and cost effective way for a CSP to satisfy this standard?

The smart card is the primer solution. It is far less expensive and captures far more data than any other option. The smart card is proven technology, and the CSP in a SSUTA context is a proven legal structure. Merging them in a CSP/ smart card solution makes a great deal of sense.

The only competing option is for the government to do it directly. However, even the German research teams working on the smart card project concede that direct government involvement compromises the effectiveness of the solution. The real-time collection of tax data by the government is not acceptable to business. However, under the SSUTA, this has not been a problem because a trusted third party does it.

CONCLUSION

SSUTA was born as an inexpensive, voluntary regime to streamlined sales tax compliance. It extends audit immunity to taxpayers who used CSPs, because the CSP is trusted by the government. A SSUTA-like system to prevent Zappers and Phantom-ware applications in ECRs could be made mandatory for all sectors of an economy or it could be applied only in high risk sectors or it could be made mandatory for taxpayers who had previously been found to manipulate sales records.

Thus, we may have a solution to Zappers and Phantom-ware at hand. If an SSUTA extension was adopted to certify ECRs, a state would not only enhance revenue and the accuracy of business records, it would gain valuable allies in the fight against tax fraud when the accuracy of business records aligns with certain personal and business interests.

Notes

[1] For more detailed discussion of Zappers and Phantom-ware see Ainsworth (2008a, 2008b, 2008c).

[2] *U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman* (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).

[3] Personal e-mail communication, Gilles Bernard, Adjunct Director General for Fiscal Research, Revenue Quebec November 24, 2008 (on file with author).

[4] The director, Mr. Apostolos Mandaltsis, was personally fined $65,681.00 and $10,300 respectively for PST (Provincial Sales Tax) and GST (federal Goods and Services Tax). Taxes and interest were due in addition.

[5] Revenue Quebec (2005b).

[6] The breakdown is: $429,179.07 (GST) + $492,023.11 (PST) + $214,589.55 (federal penalties) + $625,028.89 (provincial penalties) + $55,250.28 (judicial fees). Revenue Quebec (2003b).

[7] Revenue Quebec (2005c), additional penalties of $22,513.19 under the GST and QST, as well as income tax of $17,297.08 and related penalties of $26,621.35.

[8] *Turcotte v Quebec* (1998). This case involved the MRQ investigation of Gamma Terminal, Inc., a wholly owned Canadian subsidiary of an American company, Gamma Micro Systems. This investigation began in 1997 and focused on the distribution of the Gamma Restaurant Management System. It eventually lead to a number of conviction of restaurants that used this system to delete sales records, including the companies 136530 Canada, Inc. and San Antonio's Grill. Revenue Quebec (2005a)

[9] Bergeron and Ainsworth (2008); on file with author.

[10] Bergeron and Ainsworth (2008, p. 13); but noting further that the 16 percent figure measures all skimming frauds, not just skimming with Zappers.

[11] Revenue Quebec (2008). See also the accompanying powerpoint presentation, Tax Evasion in Quebec : Obligatory Billing in the Restaurant Sector – Under-declaration of revenues in the restaurant sector, 3 (January 28, 2008) (in French — translation on file with author).

[12] Working Group on Cash Registers (2005) (in German — translation on file with author).

[13] Working Group on Cash Registers (2005, p. 5) listing the following attributes: (1) erasing all data entries, (2) resetting the zero counter, (3) unwarranted counter-entries, (4) unwarranted use of the training mode, and (5) suppressing the grand total memory.

[14] Working Group on Cash Registers (2005, p. 5). BHR comments 2003, No 54, Federal Parliament circular 15/2020.

[15] Working Group on Cash Registers (2005, p. 5). BHR comments 2003, No 54, Federal Parliament circular 15/2020.

[16] *United States of America v. Noah Ryan Robinson and John Anthony Robinson* (1993).

[17] The Secure Hash Algorithm (SHA-1) was developed by the U..S National Institute of Standards and Technology. SHA-1 is a widely accepted data encryption tool. It produces a 40-character string by hexadecimal symbols (20 bytes), and the string [or the "hash value"] uniquely defines the processed data [in the case of an ECR issuing receipts in B2C transactions this data is the values on the printed receipt]. SHA-1 is described in detail in the Federal Information Processing Standard 180-2 (2002).

[18] CRC-32, or cycle redundancy check, takes as input a data stream of any length, and produces as output a value of a certain space, commonly a 32-bit integer. The term CRC is often used to denote either the function or the function's output. A CRC can be used as a checksum to detect alteration of data during transmission or storage. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channels.

References

Ainsworth, Richard T.

Zappers: Tax Fraud, Technology and Terrorist Funding. Boston, MA: Boston University School of Law, 2008a. Working Paper 08-07. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1095266

Zappers & Phantom-Ware: A Global Demand for Tax Fraud Technology. Boston, MA: Boston University School of Law, 2008b. Working Paper 08-20. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1139826

Zappers and Phantom-Ware at the FTA: Are They Listening Now? Boston, MA: Boston University School of Law, 2008c. Working Paper 08-21. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1147023

Bergeron, Dave and Richard Ainsworth. Zappers (Automated Sales Suppression) 12. Presentation at the New York Prosecutors Training Institute, Syracuse, NY, 2008.

Finance Quebec. 2006-2007 Budget: Additional Information on the Budgetary Measures. Montreal, QC, 2006.

Revenue Quebec.

Mr. Marcel St. Louis de l'Outaouais Convicted of Tax Evasion Related to the Use of a Zapper. News release (in French only). Quebec, QC, 2003a.

All Stratos Restaurants Convicted of Fraud in Connection with the use of a Zapper. News release (in French only). Quebec,QC, 2003b.

Fines of More Than One million Dollars – A Father and His Two Sons Convicted for Tax Evasion in Connection with the Zapper. News release (in French only). Quebec, QC, 2003c.

Tax Evasion: The Ministry of Revenue Suspects the Restaurant Grill San Antonio de Laval of Having Used a Zapper. News release (in French only). Quebec, QC, 2004.

Deux sociétés coupables d'avoir utilisé un camoufleur de ventes dans des restaurants de Laval et de Repentigny [Two companies guilty of having used a camoufleur sales in restaurants in Laval and Repentigny]. Press release (in French). Quebec City, QC, 2005a.

Revenue Quebec Investigation of a Software Designer Outlet Suspected of Having Developed and Distributed Zappers. News release (in French only). Quebec, QC, 2005b.

The Zapper Designer of Boucherville Pleads Guilty to Various Charges Brought by Inland Revenue Quebec. News release (in French only). Quebec, QC, 2005c.

The Company Audio LP, Inc. Convicted of Tax Evasion (on the conviction fines were imposed of $12,475). News release (in French only). Quebec, QC, 2007.

Pour plus d'équité dans la restauration : il faut que ça se passe au-dessus de la table [For more equity in the restaurant sector it is required that (business is conducted) above the table)]. Press release, Jean-Marc Fornier. Quebec, QC, 2008.

Turcotte v Quebec (Ministry of Revenue) 1998 CarswellQue 1041, [1998] R.D.F.Q. 110 Superior Court of Quebec.

United States of America v. Noah Ryan Robinson and John Anthony Robinson, 8 F. 3d 398 (1993)

U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994).

U.S. Department of Justice. Eastern District of Michigan.

LaShish Financial Manager Sentenced for 18 months for Tax Evasion. Press release. Detroit, MI, 2007a.

Superseding Indictment Returned Against LaShish Owner. Press release. Detroit, MI, 2007b. http://www.justice.gov/tax/usaopress/2007/txdv072007_5_30_chahine.pdf

U.S. National Institutes of Standard and Technology. Federal Information Processing Standards Publication 180-2. Washington, D.C., 2002. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

Working Group on Cash Registers. Interim Report 5, Berlin, Germany, 2005.