Zappers:
What’s Already Here?
What's Coming?

Richard T. Ainsworth
Midwestern States Association of Tax Administrators
August 27, 2012
JUMP START by Robb Armstrong

You're gonna like this movie, Jojo

It's called "Back to the Future Part Two"

It's about a kid who visits 2015...

Then he goes back to 1955 to save 1985 from disaster

Made me want a time-travelling Delorean!

Cool movie, right?

Wow. Really? No iPhones or iPads in 2015?
Who are these guys?
Prometheus & Epimetheus

• Epimethean:
  – Where have we been? ECRs/POS systems ... audit on the business premises
  – Zappers, phantomware

• Promethean:
  – Where are we going? tablets/phones/hand-held devices ... the cloud
  – Where will the next generation of Zappers be?
INDEX

• Theme: Market-place
• Estimated Losses
• Epimethean:
  • Phantom-ware
  • Zappers
  • Is there a Zapper here?
    – Ohio (Example 1)
    – Pennsylvania (Example 2)
    – Questions from the field ...

• State Legislative Activity
• Promethean:
  • Zappers in the cloud
  • Zapped credit cards
  • Zapping with tablets/phones/hand-held devices
Theme: Market-place

This is a Mid-size business issue

(1) Skimming has been an individual fraud issue, not a market-place issue

(2) Phantom-ware applications show skimming entering the market-place:
   - Self-help phantom-ware
   - Factory-installed phantom-ware

(3) Zappers developed next
   - Installers, rogue developers, smaller developers

(4) Internet based programs
**THE COMPETITIVE MARKET-PLACE**

Greece – 10m people; 800,000 SMEs; 300,000 to 350,000 ECRs and POS systems; turnover of 30,000 to 40,000 systems per year; 300+ different machines (all certified); 50 importers and manufacturers – Germany & Italy (EU); USA, Japan, China (non-EU).

**AND** Greece has the highest fraud ratio in the EU (30%)
Estimated Losses & Efforts Undertaken

1. Estimated tax losses [restaurant only] Missouri:
   - GDP = 98% of Quebec
   - $417 million

2. Total USA $21.095 billion

3. Other states:

<table>
<thead>
<tr>
<th>State</th>
<th>Loss (in billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>California</td>
<td>$2.8b</td>
</tr>
<tr>
<td>Illinois</td>
<td>$1.075b</td>
</tr>
<tr>
<td>Kansas</td>
<td>$195.5m</td>
</tr>
<tr>
<td>Nebraska</td>
<td>$132m</td>
</tr>
<tr>
<td>Iowa</td>
<td>$208m</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>$400m</td>
</tr>
<tr>
<td>Minnesota</td>
<td>$30m</td>
</tr>
<tr>
<td>New York</td>
<td>$1.8b</td>
</tr>
<tr>
<td>Michigan</td>
<td>$740m</td>
</tr>
<tr>
<td>North Dakota</td>
<td>$43m</td>
</tr>
<tr>
<td>South Dakota</td>
<td>$51m</td>
</tr>
<tr>
<td>Ohio</td>
<td>$880m</td>
</tr>
<tr>
<td>Indiana</td>
<td>$446m</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>$208m</td>
</tr>
</tbody>
</table>
Three US Zapper Cases & more?

- Connecticut case – 1994
  - Custom made zapper (former NCR IT expert)
  - Zapper is kept in a hollowed out book in office
  - $17m (IRS income tax audit) – Customs uncovered

- Michigan case #1 – 2007
  - Zapper kept at owner’s residence connected to ECRs at 13 restaurants
  - Skim $20m (4 years) sent to Hezbollah (Lebanon)
  - CIA mole (sister-in-law); wife in prison
  - Husband is fugitive from US (in Lebanon)

- Michigan case #2 – 2011
  - Installer (Journal Sales Remover program)
  - 2 strip clubs – over $500,00 gross sales
  - 5 years in prison (plea bargain – will talk
Phantom-ware

There are two types:

Self-help
Factory Installed
Type 1 – Self-help Phantom-ware

• Modern ECRs can be re-programmed to eliminate the audit trail (critical records)
  • Z Reports (daily/periodic) – end of day report that records sales, taxes, media totals, discounts, voids, etc.
  • X Reports – same as Z Reports except they do not “reset” the system after being taken.
  • Electronic Journal – records all transactions (blow-by-blow) entered in the machine

• Programming is “secret” (not in user’s manual) – limit access [bad employee issues]
Type 2 – Factory installed Phantom-ware

• Does not require re-programming

• Secret (hidden) functionality built in to ECR
  • Not discussed in user’s manual
  • Not visible in menu structure
  • Commonly revealed only in oral communications with
    » Installer
    » Sales representative

• The idea is to remove the need to re-program
  – Manufacturer loses “deniability”
  – These programs have only one function
Zappers

There are three generations
Zappers Past; Zappers Present;
Zappers Yet to Come
Zapper from the Past

• This is an old Quebec Zapper. It has been “hard wired” into the ECR. The picture shows the top of the ECR removed, and the yellow arrow points to the device.

• When Zappers are added to ECRs this way it is very easy to find them.

• People only do it this way in jurisdictions that are not looking for them.
Contemporary Zapper

Note: this Swedish zapper requires a lot of manual intervention.
A specific brand of cash register (blood)

Manufactured in Paris (since 1983)
Popular in Italy, Belgium, Portugal, Spain, Germany, Denmark, Australia, USA and North Africa.
Uses “Specific kind of” back-office program
Cash register is connected to a PC (in the back office) like the one on the following slide.
Notice the “dongle” (grey memory stick) protecting proprietary program
Notice the silver memory stick – this is the “zapper”
Restodata is programmed to automatically download all information about all transactions from all cash registers every morning at (for example) 5:00 am
Ohio
US District Court, Northern District of Ohio, Western Division
3:12-cr-262-DAK (filed 5-22-2012)

• 18 people indicted - $3 million [Tarek Elkafrawi]
• FBI; ICE-HSI; Joint Terrorism Task Force [Egypt; Jordan; Lebanon]
• Change in POS (2010) – Internet access
• Two franchise fees [Equipment/land; royalty/advertising = 8% net sales].
• Manipulation of
  – Sales, payroll, false SSN, multiple SSN, 200+ illegal workers, underpaid for overtime, “New” system manipulation of hours worked, weekly central administration credit $2,300
  – Remote access to Ohio “new system” with “specific on-line software viewer” software from home computers – reset clock; manipulate cash transactions because tickets remained open; “new system” taken “off-line”
PA & NJ
US District Court, Eastern District of Pennsylvania
2:12-cr-241-MAM (May 16, 2012)

• Evasion began in 1986 – FBI & IRS-CI
  • Philadelphia, PA area & several NJ locations
• $15 million skimmed ($2.2m income tax)
• Paid workers in cash – cash taken to Florida retirement home & kept in safes on premises
• Second set of books found
• Family owners and managers at each location
• Several owners filed $0 returns with claims for refundable credits
Calls from the field -- Zapper?

“We have an account where the records show only receipts for certain times of the day, the other times of operations are missing. I assume this would be turning off the machine or putting it on training mode. Have you heard of a zapper that would remove certain time periods from records? Thanks.”
A Possible Zapper?

“There is a chain of five restaurants in the same town, two high end, three middle to higher end. Labor ratio is 26 percent, should be around 38 to 40, mostly credit cards, seems high though the average is about 88 percent on preliminary analysis, same POS. I suspect that maybe credit cards could be diverted, need to dive deep to see what is there, the labor is out of line based on analysis of what we usually see.”
How about here?

“Another one, we have the electronic data and the order numbers are missing throughout the audit at a rate of 11 percent per quarter. Guest check numbers are missing at a smaller rate, the order numbers are deep programmed where there are reasons for missing guest receipt numbers to be missed per software IT folks, they say order numbers should always show, .... zapper?”
I was able to see a zapper in person, interesting. I can not believe how easy it works.”

- Icon [double click] + password
- Eliminate manually or automatic
- Maybe ... 10 min.
- All ECRs must be off to re-index
- Installer identified (installed in 2008)
- Owner showed how it works
- Proof of deficiency difficult ... estimates ... will pay in full
- Will use Zapper for training ...
  - Internally ...... and on the road .....
## State Legislative Activity 9/15

<table>
<thead>
<tr>
<th>STATE</th>
<th>BILL</th>
<th>ACTION</th>
<th>STATE</th>
<th>BILL</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT</td>
<td>HB 5421</td>
<td>Law</td>
<td>NC</td>
<td>SB 854</td>
<td></td>
</tr>
<tr>
<td>FL</td>
<td>HB 7099</td>
<td>Veto</td>
<td>NY</td>
<td>SB 2854</td>
<td></td>
</tr>
<tr>
<td>GA</td>
<td>HB 415</td>
<td>Law</td>
<td>OK</td>
<td>HB 2576</td>
<td>Law</td>
</tr>
<tr>
<td>IL</td>
<td>HB 6155</td>
<td></td>
<td>TN</td>
<td>SB 2194</td>
<td></td>
</tr>
<tr>
<td>IN</td>
<td>HB 1337</td>
<td></td>
<td>UT</td>
<td>HB 96</td>
<td>Law</td>
</tr>
<tr>
<td>LA</td>
<td>SB 616</td>
<td>Law</td>
<td>WV</td>
<td>SB 411</td>
<td>Law</td>
</tr>
<tr>
<td>ME</td>
<td>LD 1764</td>
<td>Law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MI</td>
<td>SB 768</td>
<td>Law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MO</td>
<td>SB 840</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Epimethean Solutions

• Comprehensive Technology
  • Greek government – certification of each ECR ($ ??)
  • German government – INSIKA smart card ($50)
  • Quebec government – Sales Recording Module ($800)
  • Private sector – Sales Data Recorder with mobile ($350)
    – Belgium; Sweden; Slovenia; Rwanda; Kenya;

• Traditional
  • Netherlands – persuasion
  • Norway – comprehensive regulation
    – Potentially like the Greek solution
Promethean Problems

• Technology solutions require a receipt
  http://www.skatteverket.se/privat/kvitto/webbfilmmedengelsktext.4.71004e4c133e23bf6db80003181.html

• Internet-based Zappers [Zapper-as-a-Service]
  – Six cases in Portugal

• Zappers have migrated into credit cards
  – United Kingdom, Portugal & Norway

• tablets/phones/hand-held devices
  – The ECR is a dinosaur
  – Big retail store #1, #2 & Big hardware store #1, #2 and Big coffee store #1 ...
Promethean Solutions

• Penalize the Installer
• Do a sting with a false restaurant
• If there are privacy concerns with comprehensive technology solutions, opt for
  – severe (limited) enforcement (Oklahoma)
  – broad (conditional) enforcement (Missouri)
  – “bad apple” enforcement (New York)
• Split credit card payments
  • Ecuador, Russia, Turkey, Argentina, Brazil, Peru, Chile, Uruguay, Austria, Mexico, Colombia, Guatemala, El Salvador, Dominican Republic, and Costa Rica.
Croatia (3)

Obavezni sadržaj računa:

- OIB
- Naziv
- Datum i vrijeme
- Redni broj računa
- Stavke kupnje
- Način plaćanja
- Obračun poreza
- Oznaka operatera (osoba)
- Zaštitni kod izdavatelja računa
- Potvrda Porezne uprave o online primitku transakcije (JIR) ili u offline modu posebna poruka - upozorenje

<table>
<thead>
<tr>
<th>ABECE d.o.o.</th>
<th>Naziv: ABECE d.o.o.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boškovićeva 5, Zagreb</td>
<td></td>
</tr>
<tr>
<td>OIB: 500563289500</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RAČUN broj</th>
<th>Naziv</th>
<th>Kol.</th>
<th>cijena</th>
<th>iznos</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000102456789</td>
<td>Kava s mljekom</td>
<td>2</td>
<td>8,00</td>
<td>16,00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UKUPNO:</th>
<th>Naziv plaćanja:</th>
</tr>
</thead>
<tbody>
<tr>
<td>16,00</td>
<td>novčanica</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Obračun poreza</th>
<th>Oznaka osobe koja je izvršila naplatu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oznaka operatera: Elagejnik 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zaštitni kod izdavatelja računa:</th>
<th>YXC1-455A-W234-55AB-OBE10987</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Porezna uprava:</th>
<th>KRFH-5DBZ-049A-OIB9</th>
</tr>
</thead>
</table>
Prometheus & Epimetheus
Further Reading

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

• Zappers & Phantom-Ware: A Global Demand for Tax Fraud Technology

• Zappers: Tax Fraud, Technology and Terrorist Funding
Thanks

• Richard T. Ainsworth

• ADP
  – Richard.Ainsworth@adp.com

• Boston University
  – vatprof@bu.edu
Supplemental Slides

• Details of a Zapped transaction (from a Swedish Zapper)
  – 11 slides

• 9 Ways to find a Zapper
  – 11 slides
Supplement 1

Details of a “zapping” from Sweden
So, before manipulation here is the electronic journal
the sales report
the sales receipt
Electronic Journal (before manipulation)

1. Item number 21 is a Lunch B
2. It cost 65,00 kroner
3. The receipt is number 2/1
### Sales Report (before manipulation)

We need this for comparison later
Sales receipt (before manipulation)

These are in the “.TIC” files (for “tickets”). Notice:

1. Item number 21
2. Sales price of 65,00 kroner
3. Ticket number (receipt number) 2/1
To manipulate the data you insert the zapper (silver memory stick)

There is a new version of the CMDCAR.DLL program on the zapper
Double-Click on the secret module

It is not all that apparent what you need to do here, but by double clicking in the box in the lower left, entering an ID and a password, you will get to the next screen – the Electronic Journal (which can be adjusted).
“Manipulate-able” Electronic Journal

Notice that we can either
(1) select a ticket to adjust, or
(2) auto-replace

So, assume we take the selection of a ticket approach … (1),

When we select the first item (ticket number 2/1) we then get …
Manipulated Electronic Journal (pro-forma)

Here is what we have done so far – is this enough manipulation?
Ticket 2/1 has been changed from 65.00 to 45.00 with a reduction of 20.00 on this ticket
There is a running total kept (in case you want to remove more)
Replace the Lunch Buffet (65,00) – with a beer (45,00)

Notice the price reduction (we could have gone lower) – Notice the tax reduction
The Swedish VAT is at 25%
Comparison: Original & Manipulated Electronic Journal

Notice the reduction in gross sales & the reduction in tax. If this record is tied into inventory control, adjustments in related purchases will be necessary [some zappers will do this for you] because you may have just “sold” more beer than you ordered.
Comparison of the TIC-files – Manipulated & Original

Notice the “?” in the Manipulated version in contrast with the letters “H”, “I” & “P” in the original version. This one of the tell-tale signs of manipulation in this particular program. It may indicate that the system has not been correctly updated since the manipulation procedure.
9 Ways to find a Zapper
How do you find Sales suppression devices?

• 1. Stealth visits before audit
• 2. Set up a dummy store
• 3. Detailed examination of ECR printouts
• 4. Concentrate on “high risk” businesses
• 5. Audit lead from a different “rigorous audit”
• 6. Audit lead from another jurisdiction
• 7. Find and follow the corrupt installer
• 8. Work collaboratively with absent owners
• 9. Read the 250 Quebec cases in your spare time to learn the fact patterns ... and other stuff ...
1. Stealth visits before audit

• This is how Revenue Quebec found its first Zapper in 1997

• Auditor visited a restaurant before opening an audit, saved her receipts, and looked for records in the TIC files of the ECR.

• Requires some luck
2. Set up a dummy store

• This is what the Canadian Broadcasting Corporation did in Montreal.

• ECR salesman approached CBC and explained factory-installed Zappers
  • Company was subsidiary of a US ECR distribution business
  • Salesmen actually gave interviews to CBC

• Connecticut has reported the similar activity in complaints by “honest” ECR sales people
3. Detailed examination of ECR printouts

- **Swedish approach**
  - There is a Swedish ECR lab in the government’s training facility that has a number of corrupted ECRs for practice & training of auditors

- **South Carolina attorney looking for this kind of evidence in court case**

- **Requires knowledge of ECR programs** – they are specific to ECR types not generic
4. Concentrate on “high risk” businesses

- Not:
  - If Mom or Pop runs the cash register
  - If publicly held enterprise

- Yes:
  - If multiple locations with a remote but actively engaged owner [La Shish (Detroit); Ronan (Australia)]
  - Employees are paid wages under the table
  - Unusual ratio of cash-credit transactions
5. Audit lead from a different “rigorous audit”

• Zappers leave a cash hoard that is difficult to dispose of – don’t stop with the initial audit, push to find the Zapper:
  • Audit shows that many employees are paid in cash [Dudok (Netherlands)]
  • Cash taken off shore- US Customs [Stew Leonard’s Dairy (CT)]
  • Cash sent to Hezbollah – Homeland Security [La Shish (MI)]
  • Normal lavish lifestyle evidence [Aleef Garage (UK)]
6. Audit lead from another jurisdiction

- Ontario picks up leads from Quebec
- New York should do the same with Quebec
- Frequently the devices spread in ethnic communities that have business ties to jurisdictions where this fraud is common [Brazil; Venezuela; Quebec]
  - Austria & Germany found similar Zappers in 600 Chinese restaurants – started in Austria with a Chinese grad student in a technology school – Germany followed the Austrian lead on audits
7. Find and follow the corrupt installer

• Revenue Quebec uses search warrants against installers simultaneously with a search of a restaurant.
  – Dudok (Netherlands) installers are correcting the system during an IRS audit to hide data
  – Boutique programmers – makers of specialty cash register programs [Roy (Quebec)]
8. Work collaboratively with “absent” owners

- Absentee owners can be victims of the management company [Celine Dion (Quebec)].
- Franchise holders [McDonalds; Burger King; Duncan Donuts] that get a royalty per sale in the store [Cincinnati, Ohio (2007) – IRS]
- A business that hires too many computer savvy students could be a victim.
9. Read the 250 Quebec cases in your spare time to learn the fact patterns

- Revenue Quebec publishes summaries of all the ongoing cases on the web.

- Go to:
What do you do when you find them?

• Think beyond the audit:
  – Who installed it?
  – Who sold it?
  – Who is competing with this business locally?

• Penalize beyond the audit:
  – Make the sale, possession, distribution of a sales suppression device punishable
  – Make continuation of the business contingent on the installation of certified ECRs [business licensing requirements]

• Contact the marketplace:
  – Treat the fraud as the tip-of-the-iceberg – let the market know you are serious
  – Initiate contact with other jurisdictions to collaborate