8-27-2018

Taxing & Zapping Marijuana: Blockchain Compliance in the Trump Administration Part 4

Richard Thompson Ainsworth

Brendan Magauran

BU School of Law

TAXING & ZAPPING MARIJUANA: BLOCKCHAIN COMPLIANCE IN THE TRUMP ADMINISTRATION
Part 4

Boston University School of Law
Law & Economics Paper No. 18-03

Revised August 27, 2018

Richard T. Ainsworth
Boston University School of Law

Brendan Magauran

Electronic copy available at: https://ssrn.com/abstract=3239982

TAXING & ZAPPING MARIJUANA:
BLOCKCHAIN COMPLIANCE IN THE TRUMP ADMINISTRATION
Part 4

Richard T. Ainsworth
Brendan Magauran

Sales suppression fraud – exploiting insecure transactions at point [10]

At the retail level the MJ Freeway or METRC software essentially functions as a marijuana-industry-specific point of sale (POS) system.[1] It is common in retail for different industry sectors (restaurants, hotels, convenience stores, or gasoline stations) to have market-specific POS systems that are molded to fit the unique characteristics of their trade. The systems created for the marijuana industry differ only in that they have "… [an elevated] level of sophistication … [with] more technology than almost any industry out there."[2]

Mark Goldfogel created the first marijuana-specific STS inventory management/ POS system as the co-founder of MJ Freeway. According to Goldfogel, it is next to impossible to find comparable systems in any other industry, because only in the marijuana trade can the sale to a final consumer precisely identify the commercial trail that a product took to get to market. He indicates:

> Every batch of cannabis sold in Colorado has a batch number that tracks back to a specific plant and the nutrients that were added to it. The vehicle that carried the plant material and the candy bars that were made from its trim have all been accounted for.
>
> In this industry, when a dispensary enters an item into their inventory, it appears on Weed Maps, Leafly, and many other social media sites. Very few other industries offer real-time social media inventory sharing, and none were doing it four years ago. This is technology at its greatest — especially when it works!

And yet, with all this technology at its disposal, the marijuana trade remains a *cash-only* industry. This is entirely the result of the federal Drug Enforcement Administration classification of marijuana as a controlled substance, which in turn places banks and other financial institutions, at risk of violating federal anti-money laundering statutes,[3] the unlicensed money-remitter statute,[4] and the Bank Secrecy Act.[5]

Soon after the DOJ issued the now rescinded eight-point guidance under the Controlled Substances Act (CSA), the Financial Crimes Enforcement Network (FinCEN) issued companion eight-point guidance under the Bank Secrecy Act (BSA). FinCEN identified the due diligence

[1] Mark Goldfogel, *The Ugly Truth About POS in the Cannabis Industry*, CANNABIS BUSINESS EXECUTIVE – CANNABIS AND MARIJUANA INDUSTRY NEWS (April 7, 2015) *available at*: https://www.cannabisbusinessexecutive.com/2015/04/the-ugly-truth-about-pos-in-the-cannabis-industry/
[2] *Id*.
[3] 18 USC §§ 1956-57.
[4] 18 USC §§ 1960.
[5] 31 USC § 5318.

Electronic copy available at: https://ssrn.com/abstract=3239982

that financial institutions must undertake when dealing with marijuana-related businesses. The FinCEN guidance has not been rescinded. Banks must:

1. verify with appropriate state authorities that the business is licensed and registered
2. review submitted license application and related documents
3. request information about the business and related parties from state licensing and enforcement authorities
4. demonstrate comprehension of normal and expected activity of the business – products, types of customers, etc.
5. engage in ongoing monitoring of public sources for adverse information re: business and related parties
6. perform ongoing monitoring for suspicious activity and "red flags"
7. periodically update this information (with frequency to be "commensurate with the risk"
8. provide consideration of whether the marijuana-related business either implicates a Cole Memo priority or violates state law[6]

In addition, after following the eight-point guidance, there are three categories of Suspicious Activity Reports (SARs) that must be submitted when dealing with a marijuana-related business. They are a *Marijuana Limited SAR*, the *Marijuana Priority SAR*, and the *Marijuana Termination SAR*.[7]

The assessment of the Association of Certified Anti-Money Laundering Specialist, is that this creates a situation where:

> [W] hen deciding whether or not to offer financial services to marijuana businesses … members of the financial industry feel the odds are against them, because [even after they files reports] they could still be held accountable, criminally and civilly, if their marijuana business clients were found to have violated the law. … [F]inancial institutions feel they are held to a higher degree of scrutiny by federal

[6] US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) Guidance Memo, *BSA Expectations Regarding Marijuana-Related Businesses*, FIN-2014-G001 (February 14, 2014) *available at*: https://www.fincen.gov/resources/statutes-regulations/guidance/bsa-expectations-regarding-marijuana-related-businesses

[7] *Id.*, The financial institution should file a "*Marijuana Limited*" SAR if, based on its customer due diligence, it has determined that the business neither implicates a Cole Memo priority nor violates state law. The report should contain identifying information (names and addresses) of the subject and related parties, as well as a narrative section specifying that the sole reason for filing is the marijuana-related nature of the business and that no additional suspicious activity has been observed. The institution's responsibilities do not stop there; it must also file continuing activity reports with the same information, as well as details about all deposits, withdrawals, and transfers connected to the account since the previous filing.

The financial institution should file a "*Marijuana Priority*" SAR if, based on its customer due diligence, it holds the reasonable belief that the business implicates a Cole Memo priority or violates state law. The report should contain "comprehensive detail" about the subject and account: identifying information (names and addresses), details regarding the implicated enforcement priorities, and detailed financial records of the transactions involved in the suspicious activity.

The financial institution should file a "*Marijuana Termination*" SAR if it deems it necessary to terminate the relationship with the marijuana-related business in order to be in compliance with its anti-money laundering program. The institution must provide a narrative noting the basis for the termination, and if possible is urged to use Section 314(b) voluntary information sharing to alert the business' new financial service provider of potential illegal activity.

Electronic copy available at: https://ssrn.com/abstract=3239982

> regulators if they accept legitimate marijuana businesses as clients; thereby running the risk of their institution's rating being downgraded. For these reasons, many financial institutions have refused financial services to marijuana businesses.[8]

As a result, "*[m]ost* cannabis businesses do *all* of their transactions in cash …"[9] An estimated 70% of cannabis businesses have no bank accounts,[10] most marijuana businesses do not accept any credit cards,[11] and the common advice from accountants is to "keep the cash under your mattress."[12] As Stuart Leavenworth notes however, all-cash businesses and technology-based tax frauds go hand-in-hand.[13]

Example: The State of Washington

The State of Washington presents a classic example of where technology-based sales tax fraud is a known problem in cash-based businesses (notably restaurants). Washington also has, far and away, the highest tax on marijuana in the country. Given that Washington collects 47.3% of its revenue (not including local government taxes) from the retail sales tax,[14] and that technology has been the backbone of the State's economy for years,[15] one would expect that ECR/POS system security measures would be mandatory and abundant. But, Washington has nothing.

---

[8] Association of Certified Anti-Money Laundering Specialist, *The Dilemma for Financial Institutions with Providing Services to Marijuana Businesses* (2016) *available at*: http://files.acams.org/pdfs/2016/The-Dilemma-for-Financial-Institutions-with-Providing.pdf

[9] Stuart Leavenworth, *When Does Too Much Cash become a Health Risk? When You Own a Marijuana Shop*, MCCLATCHY DC BUREAU (February 7, 2018) *available at*: http://www.mcclatchydc.com/news/nation-world/national/article198941964.html

[10] Robin Abcarian, *Your Business is Legal, but you Can't Use Banks. Welcome to the Cannabis all-cash Nightmare*, LA TIMES (January 29, 2017) available at: http://www.latimes.com/local/abcarian/la-me-abcarian-cannabis-cash-20170129-story.html

[11] Sophie Quinton, *Why Legal Marijuana Businesses Are Still Cash-Only*, GOVERNING STATELINE (March 22, 2016) available at: http://www.governing.com/topics/finance/sl-marijuana-businesses.html (noting a small trend at the very end of the Obama administration in Denver, Colorado where a few local banks were beginning to accept deposits from marijuana-related businesses).

[12] Leavenworth, *supra* note 9.

[13] Leavenworth, *supra* note 9 indicates:

> Yet for government agencies, it is harder to track sales from all-cash businesses than it is for those who rely on credit cards, and it becomes tougher still when those businesses can't use banks. To pay their taxes in Sacramento, some 30 city-approved marijuana shops have to stuff cash into backpacks and duffel bags and haul it to a set location each month, kept secret for security reasons.

This paragraph expressly links to an earlier tax fraud article that makes this connection to electronic sales suppression and the use of Zappers in Quebec. Stuart Leavenworth, *That Sales Tax You Pay on your Meal? Some Restaurants Keep It, Using Illegal 'Zappers,'* MCCLATCHY DC BUREAU (December 6, 2017) *available at*: http://www.mcclatchydc.com/news/nation-world/national/article188195589.html

[14] Washington State Department of Revenue, Research and Fiscal Analysis Division, TAX STATISTICS 2016, Chart 1, *available at*: http://dor.wa.gov/Docs/Reports/2016/Tax_Statistics_2016/chart1.pdf

[15] Blanca Torres, *Washington State Ranks No. 1 for Combined Job and Wage Growth*, SEATTLE TIMES, (February 15, 2016) *available at*: http://www.seattletimes.com/business/economy/employment-and-wage-growth-in-washington-outpacing-other-states/; Washington Technology Industry Association, INFORMATION & COMMUNICATION TECHNOLOGY: ECONOMIC & FISCAL IMPACT STUDY (February, 2015) *available at*: https://www.scribd.com/document/257405449/ICT-Economic-Report-Executive-Summary-1

Electronic copy available at: https://ssrn.com/abstract=3239982

Washington knows it has a problem. The Washington Department of Revenue (DOR), Legislative Liaison, David Duvall, indicated in House Hearings on February 2, 2018 that Washington lost in excess of $1,000,000,000 over the previous four-year period from Electronic Sales Suppression (ESS) frauds.[16] The DOR projected future losses of $1,565,764,000 through FY 2023.[17]

The most common types of sales suppression technology are Zappers and Phantomware programming.[18] In some instances, sales suppression is a personal (hands-on) service offered by installers or ECR/POS sales representatives, that is, Sales Suppression as a Service or SSaaS.[19] Recently suppression technology has entered the Dark Cloud, a fully automated manipulation of sales data that (physically) takes place off shore and uses internet-based data transfers.[20] If ESS is present in Washington's marijuana supply chain, it is most likely Dark Cloud ESS.

There are no reported cases of Zappers, Phantomware, SSaaS, or Dark Cloud functionality deployed within the legalized marijuana supply chain in Washington, or in any State, but all of the warning signs are up and flashing. Marijuana is a high value/ low volume good, being sold almost exclusively for untraceable cash, within a high-tax, technologically sophisticated commercial environment that has traditionally been closely associated with organized crime. If we assume that ESS devices are installed or operational in Washington State's marijuana dispensaries as they are in an estimated 30% or more of its restaurants,[21] then what would this fraud look like?

Fraud Patterns

A marijuana dispensary is like a normal retail establishment. It can sell both taxable marijuana and regularly taxable items (like business-name promotional T-shirts). Non-taxable items could be sold as well. ESS allows sales to be initially recorded in a POS system, a receipt

[16] Washington States House Finance Committee Working Session: *Sales Suppression* (February 2, 2018) at time mark 4:40, *available at*: https://www.tvw.org/watch/?eventID=2018021039;
[17] Washington State DOR, David Duvall, *Sales Suppression Software* (powerpoint) slide 3 (February 2, 2018) available at:
https://app.leg.wa.gov/CMD/document.aspx?agency=3&year=2018&cid=1624&mid=28040&hid=219254
[18] Richard T. Ainsworth, *Zappers and Phantomware: The Need for Fraud Prevention Technology*, 50 TAX NOTES INTERNATIONAL 1017 (June 23, 2008); Richard T. Ainsworth, *Zappers and Phantomware: Are State Tax Administrators Listening Now?* 49 STATE TAX NOTES 103 (July 14, 2008)
[19] Richard T. Ainsworth, *Sales Suppression as a Service (SSaaS) and the Apple Store Solution*, 73 STATE TAX NOTES 343 (August 4, 2014).
[20] The Dark Cloud is a term coined for this discussion. As with the Phantomware term, there comes a time in this analytical effort where an activity is becoming common enough that a new term is needed. A Dark Cloud is an anonymous internet business which accepts data transmission from ECRs or POS systems, manipulates sales data with pre-determined algorithms on a specified schedule, and then returns the data to the systems from which it came. Dark Clouds operate both on a regular schedule (daily, weekly, monthly) or on a real-time basis. They have appeared in the New York and North Carolina markets. There is no evidence of Dark Clouds operating in the State of Washington (yet). The term is unrelated to and unintentionally borrowed from the old Japanese action role-playing video game *Dāku Kuraudo* developed by Level-5 and published by Sony Entertainment around 2000.
[21] Depending on the jurisdiction, and the research study consulted, ESS is estimated to be present in 34% (of Canadian), 50% (of German – two studies), and 70% (of Swedish and Slovenian) businesses. Richard T. Ainsworth & Robert Chicoine, *Washington's Problematic Sales Suppression Enforcement Regime*, __ STATE TAX NOTES _ (forthcoming, March 19, 2018) at n. 3, 4, 5, & 6.

Electronic copy available at: https://ssrn.com/abstract=3239982

issued, taxes imposed, and collected, but then have certain transactions modified or eliminated after sales are completed. Fraud patterns could include:

- Selling recreational or medicinal marijuana to a consumer, collecting the tax, but having an ESS device delete the sale from the system;
- Selling recreational marijuana to a consumer (taxed at a 47% rate), but having the ESS device change the sale from recreational to medicinal (taxable at 37% – that is, exempt from the retail sales tax);
- Selling recreational marijuana to a consumer (at a 47% tax rate), but having an ESS device change the sale from recreational marijuana to a taxable T-shirt sale (taxed at a 6.5% rate);
- Selling recreational or medicinal marijuana to a consumer (taxed at a 47% or 37% rate), collecting the tax, and recording the sale, but where the actual product comes from smugglers. In this pattern the smuggled inventory is un-recorded (that is, not included in earlier reports to the State). The ESS device will simply eliminate the entire transaction from the business records. The source of the smuggled supply can be one of the following:
    - Excess "home grown" marijuana cultivated within-the-state, but outside of the METRC system;
    - Excess marijuana un-reported to the State, because it is part of the estimated 50% of cultivated plants that do not grow well and are deemed to be "discarded" at the farm level;
    - Excess marijuana un-reported to the State, because it is part of the estimated 35% of quality defects ("waste products") cast off during the manufacturing process, and that are deemed to be "discarded" at the manufacturer level;
    - Smuggled excess "home grown" marijuana from another State, most likely from a State with a liberal limit on "home grown" marijuana (probably for medical use);
    - Smuggled marijuana from outside the US.

Solutions

ESS has the ability to turn the Retailer in the basic marijuana supply chain into a platform for illegal distribution. ESS allows legal and illegal marijuana to be sold side-by-side for quick cash.

There are well established solutions to ESS. The solutions are technology-intensive and can be adopted country-wide (see Rwanda[22] and more recently Fiji[23]) or limited to a specific industry (see Quebec's security mandate in the restaurant sector[24]). The solutions guarantee that all sales information reaches an independent ratification service, which provides the issuer with a response that digitally confirms the sales information, and which allows asynchronous

[22] Eva Ghirmai et al., *The Incidence and Impact of Electronic Billing Machines for VAT in Rwanda*, INTERNATIONAL GROWTH CENTER BLOG (April 15, 2016) available at: https://www.theigc.org/blog/the-incidence-and-impact-of-electronic-billing-machines-for-vat-in-rwanda/ Richard T. Ainsworth & Goran Todorov, *Stopping VAT Fraud with DICE – Digital Invoice Customs Exchange*, 72 TAX NOTES INTERNATIONAL 637 (November 18, 2013)

[23] Fiji Revenue and Customs Service, *Electronic Fiscal Device (EFD)/ VAT Monitoring Systems (VMS) Update* (September 29, 2017) Press Release 48/2017

[24] Richard T. Ainsworth & Urs Hengartner, *Quebec's Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud with Technology* 57 CANADIAN TAX JOURNAL 715 (2009)

Electronic copy available at: https://ssrn.com/abstract=3239982

verification of that sale. This process of sharing sales information data will occur regardless of outside circumstances. The verification service must be available at any time and at any place.

Stated another way, a well-designed anti-ESS system will contain at least the following eleven elements:

1. A POS system must produce a document (receipt or invoice) with sufficient transactional data to confirm the proper tax calculations;
2. The document must be safeguarded with an electronic signature produced by a secure element that uses encryption to confirm authenticity and is free from manipulation;
3. The secure element used for signing the document must be independent of the creator of the POS system's tax calculation engine;
4. The secure element and invoice system must be available in any place and at any time;
5. The secure element and invoice system must work together smoothly, avoiding any delay in document production;
6. The document must clearly identify the issuer;
7. A simple document inspection must immediately provide payment information;
8. Simple inspections do not require authorized personnel or technical knowledge to verify encrypted data;
9. Authorized personnel will use a prescribed method to inspect the secure element from which data about all transactions can be extracted (in encrypted form);
10. Electronic journals (in human readable format) must be provided through the invoicing system (or the secure element);
11. Verification services will authenticate documents for authorized personnel and for the general public (at any time – most likely on line)

One of the most critical of these eleven elements is the third. The security provider should never be the same firm that provides the POS system. That means MJ Freeway should not be asked to secure the POS and invoice production aspects of its Leaf Data Systems. Franwell Inc. should not be asked to secure the POS and invoice production aspects of its METRC system.

There are a large number of examples where POS manufacturers that are developing apparently secure systems, are discovered to have embedded Phantomware in their systems or developed a Zapper that defeats their own visible security regime. Canada has a large number of these cases.

The Canadian example that impacts Washington immediately is the InfoSpec/Profitek POS and Zapper, which crossed the border from Vancouver around 2008.[25] More disturbing than InfoSpec/Profitek is a case out of Brazil in 2006.

A Brazilian software company [AGM Consultancy and Systems Corporation, Ltd.,] was hired to design a certified POS system (Robot) for the government. The system was mandated for use by the business community. This trusted company, under government contract

[25] Richard T. Ainsworth, *Sales Suppression: The International Dimension*, 65 AMERICAN UNIVERSITY LAW REVIEW 1241 (2016) (discussing the rise of InfoSpec/ Profitek in Canada, audit and subsequent litigation by the Canadian Revenue Authority, followed by the same cycle of audit and litigation that is still going on Washington State).

Electronic copy available at: https://ssrn.com/abstract=3239982

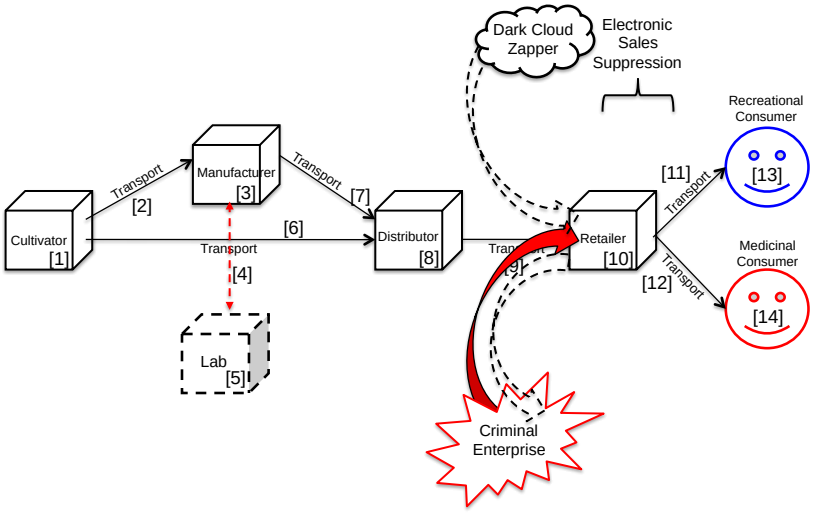
nevertheless developed and sold a Dark Cloud Zapper (Quanto) that manipulated its own POS systems from the Internet.[26]

It is reasonably clear that without a first-rate, independent, transactional security system transmitting verifiable data back to the State in real-time, that the Retailer in the basic marijuana supply chain can easily become a platform for fraud. All the Retailer needs is:

a) an ESS device (Zapper, Phantomware, SSaaS, or the Dark Cloud) that works with its POS, and
b) a supply of marijuana (Black Inventory) that had escaped the State's TAT or STS system.

The most likely scenario? Dark Cloud Zapper working with Black Inventory. See Figure 10 (below):

Figure 10:
Criminal Enterprises using the Retailer as a Platform to Sell Smuggled Marijuana to Consumers – Manipulating the Recordkeeping Function of the Retailer's POS with a Dark Cloud Zapper



Is there a Zapper that works with one of the major TAT or STS POS systems? If there is, then the most likely candidate for a vulnerable system is MJ Freeway's. Not only was the system hacked, beginning in December 2016 – leading to the cancellation of the Nevada STS contract – but the company's source code has been posted on the open net for anyone to see.[27]

Washington has first-hand experience with glitches in MJ Freeway's software. After MJ Freeway was selected in June 2017 to replace Florida-based BioTrackTHC, MJ Freeway's software had too many bugs to become operational on the November 1, 2017 contract date. The

[26] *Empresa de JF burlava o fisco via computador* HOJE EM DIA (*A JF-based Corporation defrauded the tax authorities via computer* TODAY BRAZIL) (May 12, 2006) *available at*: http://www.fazenda.mg.gov.br/empresas/ecf/noticias/hojeemdia12052006.pdf (in Portuguese) (translation on file with author) (discussing *Operation Internet* which was an effort to shut down a Dark Cloud ESS regime by the State Tax Administration of Minas Gerais, a Brazilian State in the Southeast region - close from Rio and São Paulo).

[27] See text *supra* associated with notes **Error! Bookmark not defined.** through **Error! Bookmark not defined.**.

Electronic copy available at: https://ssrn.com/abstract=3239982

transition to MJ Freeway in Washington needed two-month more months. BioTrackTHC, the firm that was being replaced, refused to assist Washington, claiming that they experienced data breaches after MJ Freeway gained access to the BioTrackTHC legacy system.[28]

In short, there is clearly enough confidential MJ Freeway code available to hackers, and there are continuing problems with security in the MJ Freeway's product to make it reliable. It is not hard to imagine that someone could assemble the kind of Dark Cloud Zapper that AGM Consultancy and Systems did in Brazil in 2006. The risk is serious.

Washington needs to mandate an advanced real-time digital security regime comparable to that recently deployed in Rwanda and Fiji throughout the basic marijuana supply chain. Based on the system installed to resolve Washington's first Zapper case involving a Settle restaurant, *State of Washington v. Wong*, Wash. Super. Ct., No. 16-1-00179-0, the cost would be roughly $10,000 to $15,000 per marijuana dispensary.

[28] Lester Black, *State's Pot Tracking Software Causes Headaches for the Legal Weed Industry*, THE STRANGER (October 24, 2017) *available at*: https://www.thestranger.com/slog/2017/10/24/25490384/states-pot-tracking-software-causes-headaches-for-the-legal-weed-industry Patrick Vo, CEO of BioTrackTHC indicated,

> … two months ago [August, 2017], an e-mail was sent to multiple licensees offering to sell the raw data behind Washington, Pennsylvania, and Nevada's recreational and legal weed markets. … proprietary data was shared in this e-mail that made it appear to show that Washington's data had been hacked.

Electronic copy available at: https://ssrn.com/abstract=3239982