

Green Marimba Technologies

3/15/2017

Payment processing services for the cannabis industry

Matt Brown, Owner, Business development
matt@greenmarimba.com

Overview

The cannabis industry, currently worth 6 billion dollars and projected to reach up to 50 billion dollars over the next decade,¹ suffers from a desperate lack of adequate financial services. While banking services are available in most states that have legalized marijuana, a major problem for cannabis businesses is finding legal, compliant, and stable services for handling electronic payments. This forces these businesses to operate primarily with cash, which entails significant security risks and raises costs for both the businesses and the banks that they use.

In this document we first examine the legal and regulatory framework under which the federal government permits cannabis products to be sold and the roles and risks of providers of financial services within it. We then explore what specific options are available to cannabis businesses for accepting electronic payments. We discuss how electronic payment processing systems work, including services that handle credit and debit card transactions and online closed-loop electronic payment services, and analyze their legality, compliance, and appropriateness for use in the cannabis industry from a regulatory point of view.

I. The current legal framework for cannabis as it pertains to financial services

The sale or purchase of cannabis products is illegal under federal law. Cannabis is currently categorized as a Schedule I prohibited substance under the Controlled Substances Act (CSA); Schedule I drugs, substances, or chemicals are defined as drugs with no currently accepted medical use and a high potential for abuse.² For it to be legalized, cannabis would have to be taken off this list, either by the attorney general via the DEA or by new legislation passed in Congress and signed by the President. Cannabis could alternatively be rescheduled to a different category of controlled substance, but purchases of any controlled substance require a prescription, which in turn requires a time consuming process for FDA approval. Neither legalization nor rescheduling seem likely at present time.

However, marijuana's illegal status is increasingly out of line with public opinion, particularly with respect to medical use. A Quinnipiac poll conducted in May 2016 found that 89% of registered voters polled agreed with the statement that "people should be allowed to use medically prescribed marijuana."³ As of December 28, 2016, 28 states – a majority – have legalized medical marijuana.⁴

In response to this disharmony between federal and state laws, James M. Cole, former Deputy Attorney General under the Obama administration, issued guidance regarding how cannabis would be regulated under that administration in 2013 in a document referred to as the "Cole Memo"⁵. Although government priorities are likely to be changed by the new Attorney General Jeff Sessions, at present time, the Cole Memo is still the foundation of federal policy on marijuana.

The Cole Memo lists 8 specific priorities that represent the federal government's concerns:

¹<https://www.bloomberg.com/news/articles/2016-09-12/cannabis-industry-to-expand-to-50-billion-by-2026-analysts-say>

² DEA website: <https://www.dea.gov/druginfo/ds.shtml>

³<http://www.politico.com/story/2016/06/do-people-support-legalizing-marijuana-223928>

⁴<http://medicalmarijuana.procon.org/view.resource.php?resourceID=000881>

⁵ Found at <https://www.justice.gov/iso/opa/resources/3052013829132756857467.pdf>

1. Preventing the distribution of marijuana to minors;
2. Preventing revenue from the sale of marijuana from going to criminal enterprises, games, and cartels;
3. Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
4. Preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
5. Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
6. Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
7. Preventing the growing of marijuana on public lands in the attendant public safety and environmental dangers posed by marijuana production on public lands;
8. Preventing marijuana possession or use on federal property.

It goes on to state the following:

“In jurisdictions that have enacted laws legalizing marijuana in some form and that have implemented strong and effective regulatory and enforcement systems to control the cultivation, distribution, sale, and possession of marijuana, conduct in compliance with those laws and regulations is less likely to threaten the federal priorities set forth above. Indeed, a robust system may affirmatively address these priorities by, for example, implementing effective measures to prevent diversion of marijuana outside of the regulated system and two other states, prohibiting access to marijuana by minors, and replacing an illicit marijuana trade that funds criminal enterprises with a tightly regulated market in which revenues are tracked and accounted for. In those circumstances, consistent with the traditional allocation of federal-state efforts in this area, enforcement of state law by state and local law enforcement and regulatory bodies should remain the primary means of addressing marijuana related activity. If state enforcement efforts are not sufficiently robust to protect against the harms set forth above, the federal government may seek to challenge the regulatory structure itself in addition to continuing to bring individual enforcement actions, including criminal prosecutions, focused on those harms.”⁶

Thus, the Cole Memo establishes that the federal government intends to leave enforcement up to the states in most cases while preserving its right to selectively prosecute cases at its sole discretion based on the stated priorities.

Because cannabis is a controlled substance, financial services provided to cannabis businesses could be construed as aiding and abetting a crime. They also could be technically considered money laundering under Title 18 of the US Code⁷. In order to clarify how the government’s position on cannabis impacts financial institutions servicing the industry, the Treasury Department’s Financial Crimes Enforcement Network (“FinCEN”), the bureau responsible for “safeguarding the financial system from illicit use and combating money laundering”⁸, has published cannabis-specific guidelines for banks.

In general and for all industries, FinCEN has long established that:

⁶ Cole Memo, <https://www.justice.gov/iso/opa/resources/3052013829132756857467.pdf>, page 3

⁷ <https://www.law.cornell.edu/uscode/text/18/1956>

⁸ <https://www.fincen.gov/about/mission>

“Financial institutions must file suspicious activity reports if the financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution: involves funds derived from illegal activity or is an attempt to disguise funds derived from illegal activity, is designed to abate regulations promulgated under the Bank Secrecy Act, or lacks a business or parent lawful purpose.”⁹

Further clarification is found in the FDIC’s Rules and Regulations Part 353 - Suspicious Activity Reports. The relevant sections are transcribed below:

§ 353.3 Reports and records.

(a) *Suspicious activity reports required.* A bank shall file a suspicious activity report with the appropriate federal law enforcement agencies and the Department of the Treasury, in accordance with the form's instructions, by sending a completed suspicious activity report to FinCEN in the following circumstances:

(1) *Insider abuse involving any amount.* Whenever the bank detects any known or suspected federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank, where the bank believes it was either an actual or potential victim of a criminal violation or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying one of the bank's directors, officers, employees, agents, or other institution-affiliated parties as having committed or aided in the commission of the criminal violation, regardless of the amount involved in the violation;

(2) *Transactions aggregating \$5,000 or more where a suspect can be identified.* Whenever the bank detects any known or suspected federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank, and involving or aggregating \$5,000 or more in funds or other assets, where the bank believes it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an "alias", then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as driver's license or social security numbers, addresses and telephone numbers, must be reported;

(3) *Transactions aggregating \$25,000 or more regardless of potential suspects.* Whenever the bank detects any known or suspected federal criminal violation or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank, involving or aggregating \$25,000 or more in funds or other assets, where the bank believes it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, even though the bank has no substantial basis for identifying a possible suspect or group of suspects; or

(4) *Transactions aggregating \$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.* Any transaction (which for purposes of this paragraph (a)(4) means a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected) conducted or attempted by, at or through the bank and involving or aggregating \$5,000 or more in funds or other assets, if the bank knows, suspects, or has reason to suspect that:

⁹<http://jux.law/the-cole-memo-and-banks/>

- (i) The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law;
- (ii) The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or
- (iii) The transaction has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.¹⁰

As selling cannabis is an illegal activity under federal law, FinCEN establishes that all financial institutions must file suspicious activity reports (SAR) for every cannabis transaction that they participate in. Since the main purpose of cannabis SAR reports is to identify whether any of the Cole Memo priorities are being violated, it provides three specific types of cannabis-specific SARs: “Marijuana Limited” filings if it does not appear that the transaction violates any of the priorities stated in the Cole Memo or state law; “Marijuana Termination” filings if the financial institution terminates its relationship with a cannabis business; and “Marijuana Priority” filings if it reasonably believes that state law or one of the Cole Memo priorities has been violated. To help clarify for financial institutions what might constitute reasonable belief that one of the Cole Memo priorities has been violated, it establishes a number of specific “Red Flags” for Priority Suspicious Activity Reports:

- A customer appears to be using a state-licensed marijuana-related business as a front or pretext to launder money derived from other criminal activity (i.e., not related to marijuana) or derived from marijuana-related activity not permitted under state law. Relevant indicia could include:
 - The business receives substantially more revenue than may reasonably be expected given the relevant limitations imposed by the state in which it operates.
 - The business receives substantially more revenue than its local competitors or than might be expected given the population demographics.
 - The business is depositing more cash than is commensurate with the amount of marijuana-related revenue it is reporting for federal and state tax purposes.
 - The business is unable to demonstrate that its revenue is derived exclusively from the sale of marijuana in compliance with state law, as opposed to revenue derived from (i) the sale of other illicit drugs, (ii) the sale of marijuana not in compliance with state law, or (iii) other illegal activity.
 - The business makes cash deposits or withdrawals over a short period of time that are excessive relative to local competitors or the expected activity of the business.
 - Deposits apparently structured to avoid Currency Transaction Report (“CTR”) requirements.
 - Rapid movement of funds, such as cash deposits followed by immediate cash withdrawals.
 - Deposits by third parties with no apparent connection to the account holder.
 - Excessive commingling of funds with the personal account of the business’s owner(s) or manager(s), or with accounts of seemingly unrelated businesses.
 - Individuals conducting transactions for the business appear to be acting on behalf of other, undisclosed parties of interest.
 - Financial statements provided by the business to the financial institution are inconsistent with actual account activity.

¹⁰<https://www.fdic.gov/regulations/laws/rules/2000-7500.html>

- A surge in activity by third parties offering goods or services to marijuana-related businesses, such as equipment suppliers or shipping servicers.
- The business is unable to produce satisfactory documentation or evidence to demonstrate that it is duly licensed and operating consistently with state law.
- The business is unable to demonstrate the legitimate source of significant outside investments.
- A customer seeks to conceal or disguise involvement in marijuana-related business activity. For example, the customer may be using a business with a non-descript name (e.g., a “consulting,” “holding,” or “management” company) that purports to engage in commercial activity unrelated to marijuana, but is depositing cash that smells like marijuana.
- Review of publicly available sources and databases about the business, its owner(s), manager(s), or other related parties, reveal negative information, such as a criminal record, involvement in the illegal purchase or sale of drugs, violence, or other potential connections to illicit activity.
- The business, its owner(s), manager(s), or other related parties are, or have been, subject to an enforcement action by the state or local authorities responsible for administering or enforcing marijuana-related laws or regulations.
- A marijuana-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.
- The owner(s) or manager(s) of a marijuana-related business reside outside the state in which the business is located.
- A marijuana-related business is located on federal property or the marijuana sold by the business was grown on federal property.
- A marijuana-related business’s proximity to a school is not compliant with state law.
- A marijuana-related business purporting to be a “non-profit” is engaged in commercial activity inconsistent with that classification, or is making excessive payments to its manager(s) or employee(s).¹¹

Therefore, federal compliance ultimately ends up being a matter of whether activities conducted within the cannabis industry raise any of these red flags. If so, banks are required to send a Marijuana Priority SAR, which could lead to a federal investigation of a given transaction, a pattern of transactions, or the bank itself.

(For a more in-depth treatment of the legal framework of cannabis in the US, see: <https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2016/08/03/changes-needed-to-protect-banking-and-financial-services-when-dealing-with-the-marijuana-industry.aspx>)

¹¹<https://www.fincen.gov/resources/statutes-regulations/guidance/bsa-expectations-regarding-marijuana-related-businesses>

II. Electronic payment processing solutions currently available

The payment processing solutions currently available to cannabis businesses fall into three categories:

1. Traditional merchant services
2. Point-of-Banking services (Cashless ATMs)
3. Closed-loop services

Traditional Merchant Services

Traditional merchant services are provided by Merchant Service Providers (MSP) or Independent Sales Offices (ISO) to handle credit and debit card transactions, either via terminals or online. Traditional merchant services are considered “online debit transactions” and require the purchaser to sign a receipt. They use proprietary networks set up by companies like MasterCard, Visa, or American Express.

Since all three of these companies have publicly announced policies of not allowing their credit cards to be used for marijuana purchases, any such use is against their rules and violations and may lead to penalties or terminated merchant status. This is also true for debit card transactions via traditional merchant services. Debit cards are issued by banks, but traditional merchant services still use MasterCard and/or Visa’s proprietary networks, and are therefore cannabis purchases made with debit cards are in also violation of their stated anti-cannabis policies. However, use of debit or credit cards for purchases of products that are not permitted by these companies’ policies or rules is not technically illegal, as it does not directly violate any US law.

While the purchase of cannabis products is illegal under federal law, the Cole Memo establishes that prosecution is not a federal priority as long as the participants in any cannabis transactions comply with state regulatory systems pursuant to the priorities stated within it. Therefore, purchases of marijuana and derivative products can be considered to be permitted by law, although technically illegal.

The relevant issue in assessing whether the use of credit and debit cards for marijuana purchases constitutes an illegal activity or not is whether or not the sale of cannabis products involves other unlawful activities.

When purchases are made with a MasterCard or Visa credit or debit card, merchant codes are assigned to each transaction that are specific to the category of product being purchased. These codes are used for internal purposes and by the IRS for tax reasons, as some types of products such as alcohol or tobacco are taxed at different rates. Because these companies do not support cannabis transactions, they have not issued cannabis merchant codes. As result, any cannabis transactions processed by MasterCard or Visa would have to use a merchant code of a different product or product category. There are three main strategies for doing this:

1. Miscoding, in which merchant codes of other products are substituted;
2. Shadow banking, in which cannabis businesses process payments in the name of another business unrelated to the cannabis industry;
3. Aggregating accounts, in order to bundle cannabis transactions in with other “legitimate” transactions.

These activities are also against Visa and MasterCard’s public policies and can lead to penalties or permanent loss of merchant services by inclusion in a Terminated Merchant File. Still, strictly speaking, these activities are not technically illegal if the product being concealed or miscoded 1) is a product that can legally be sold and purchased, and 2) there is no intent to defraud the IRS by paying a lower tax rate.

The question of whether cannabis transactions under traditional merchant services are illegal depends on how strictly the letter of the law is applied. Technically, even if cannabis’s illegal status is overlooked pursuant to the Cole Memo, all three of these strategies could be illegal under the Bank Secrecy Act (and FinCEN’s provisions to address BSA concerns within the Cole Memo), which as noted earlier establishes that any attempts to *disguise or conceal* an illegal activity are illegal. However, one could make the claim that since the federal government has chosen to permit cannabis purchases in general, the strategies described above are not in fact concealing an unlawful activity, but rather a federally permitted activity, and therefore would not be in violation of the BSA. How successful such a claim might be in a court of law is a matter of conjecture. In any case, the likelihood of federal persecution would be small due to cost effectiveness.

In any case, if any of the above strategies were definitively identified by either the issuing bank or the acquiring bank in a transaction, they would clearly have to submit Priority Marijuana SAR reports which could result in a federal investigation. Since this is undesirable to banks, their approach has often been to refuse to work with MSPs that serve the cannabis industry or to close customer accounts upon any suspicion or any investigation by credit card companies. The MSPs themselves may choose to shut down operations if they feel they are at risk of investigation. This not only disrupts the merchant’s business, but can also result in lost funds or difficulties receiving funds that are being processed.

Despite reports that Visa and MasterCard have “quietly decided not to enforce their rules and allow certain marijuana retailers to use their payment processing services for their customer purchasers as long as their merchant acquirers (banks) decide such transactions are legal,”¹² Green Marimba’s view is that traditional merchant services is an imperfect solution for the cannabis industry as they expose participants to a variety of fines, possible termination as a merchant, and the possibility (although small) of legal persecution. However, as long as there are banks and MSPs willing to serve the industry, it is ultimately the client’s choice as to whether the risks are worth it.

Cashless ATMs

A payment processing alternative to traditional merchant services is Cashless ATM solutions (also called Point of Banking systems), which are often marketed towards high-risk businesses that want to accept credit and debit cards but have difficulties getting a merchant services account. The use of Cashless ATMs by cannabis businesses was prevalent in the past, but they are less popular today, perhaps due to their perceived instability. A number of MSPs have been forced to suddenly withdraw their services,

¹²<https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2016/08/03/changes-needed-to-protect-banking-and-financial-services-when-dealing-with-the-marijuana-industry.aspx>.

Also see Robin Sidel, *Card Conundrum Develops in Colorado over Marijuana Sales*, wall St. J. (Jan. 6, 2014), <http://www.wsj.com/articles/SB10001424052702304887104579304970273466300>; David Migoya, *Recreational Pot: Processors of Credit, Debit Cards Relax Rules*, Denver Post (Jan. 8, 2014).

leaving their clients in the lurch. Among the more well-publicized instances of this are MetaBank's shutting down of hundreds of ATMs and Cashless ATMs in late 2014¹³.

Cashless ATMs, originally known as “scrip machines” or “scrip cash dispensaries”, have been used worldwide for decades and were primarily envisioned as a way to provide cash on demand in places where a traditional ATM would be cost-prohibitive due to low usage. They also reputedly last longer and require less maintenance¹⁴, as they have less moving parts. They have been much more widely used outside the US, particularly in the third world, and their success in the US has been limited “due largely to regulatory stipulations limiting processing network availability”.¹⁵

Scrip machines or Cashless ATMs operate in a manner similar to regular ATMs.¹⁶ In both cases users swipe or enter their cards, type in a pin code, and select an amount of cash to debit from their checking accounts or an amount to be withdrawn as a cash advance in the case of a credit card. In the case of a regular ATM, a machine disburses the cash. With scrip machines, users swipe a card at a terminal and receive a paper voucher or “scrip” for a given amount of cash, which could be taken to the cash register and applied towards a purchase as if it were cash. Modern Cashless ATMs connect directly to a cash register and dispense with the vouchers, but the transactions are still recorded as cash transactions and appear in consumers' bank account statements as cash withdrawals. As with normal ATMs, amounts to be debited have to be in increments of five dollars and typically consumers debit amounts slightly over the amount of the purchase and receive a small amount of change at the register.

Initially scrip machines were treated in the industry as functionally equivalent to ATMs. According to Wikipedia, “Some national banking regulators, such as the US Federal Reserve, define ATM transactions simply as electronic access to one's checking account and makes no distinction or mention of the location of the vault or cash drawer”.¹⁷ It also says, “In order to allow a more diverse range of devices to attach to their networks, some interbank networks have passed rules expanding the definition of an ATM to be a terminal that either has the vault within its footprint or utilizes the vault or cash drawer within the merchant establishment. This allows for the use of scrip cash dispenser transactions to be conducted in a similar manner to ATMs.”¹⁸ However no citations were provided.

It appears that use of Cashless ATMs have been in steady decline in the US due to increasing problems getting access to the networks they need to run on. As of 2004, Cashless ATMs could run on ATM networks or on POS networks and there were perhaps 10,000 in use in the US. However it seems that about that time merchants began to be pushed out of ATM networks “because networks prefer that scrip machines operate on standard POS networks”.¹⁹ Unfortunately, there are some reports that decline rates for Cashless ATMs on POS networks are as high as 50%.²⁰ For some reason, about that time ATM networks began terminating Cashless ATM merchant accounts.²¹

¹³<http://www.denverpost.com/2014/10/23/hundreds-of-atms-unplugged-in-legal-pot-shops-in-colorado-washington/>

¹⁴<https://www.atmmarketplace.com/articles/scrip-machines-scratch-and-scrape-for-a-piece-of-the-atm-market/>

¹⁵<https://www.atmmarketplace.com/blogs/will-cashless-atms-ever-pay-off-for-iads/>

¹⁶<https://www.cardpaymentoptions.com/credit-card-processing/marijuana-merchant-services-providers/>

¹⁷https://en.wikipedia.org/wiki/Scrip_cash_dispenser

¹⁸https://en.wikipedia.org/wiki/Scrip_cash_dispenser

¹⁹http://www.greensheet.com/gs_archive.php?issue_number=040402&story=12

²⁰http://www.greensheet.com/gs_archive.php?issue_number=040402&story=12

²¹http://www.greensheet.com/gs_archive.php?issue_number=040402&story=1

Also, MasterCard and Visa have refused to support Cashless ATMs. ATM operators compete with credit card companies; an antitrust lawsuit recently went before the Supreme Court “accusing Visa, Mastercard, and several U.S. banks of conspiring to inflate the prices of ATM access fees in violation of antitrust law”.²²

In the US, scrip machines use has generally been restricted due to network limitations to regional networks primarily found in the Southern and Eastern US.²³ According to one source, “Since the early 1990s, key U.S. industry manufacturers and IADs have ceased endeavors to sell cashless ATMs due to stringent processing regulations from MasterCard and Visa, and shrinking availability of regional networks supporting scrip.”²⁴ According to Jonathan Johnson, vice president at International Merchant Services, “Scrip was a fantastic product, and the technology would have succeeded if MasterCard and Visa did not have rules against it... Regional networks alone were not enough to keep the transactions flowing. Many regional networks no longer allow scrip and some processors have even removed support.”²⁵ (2012).

Notwithstanding their lack of popularity and diminished geographical range, there are still a number of merchant service providers that provide Cashless ATM solutions to the cannabis and other industries. Where the networks support them and whether or not they will continue to do so is difficult to determine.

The unlicensed money transmitter statute of the U.S. Code (18 U.S.C. § 1960) establishes that, “Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both... (where)the term “unlicensed money transmitting business” means a money transmitting business which affects interstate or foreign commerce in any manner or degree and(a) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable; (b) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or (c) **otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity...**”²⁶(emphasis mine). Therefore, we should establish in the first place that for a Cashless ATM service to be legally operable, it should be licensed as a money transmitter in the state in which it is operating. Second, point (c) would appear to categorize cannabis transactions via any electronic payment processing service as illegal; however, the notion of what constitutes “unlawful activity” is blurred by the Cole Memo. While technically illegal, the fact that the federal government has permitted cannabis to be traded essentially turns “unlawful activity” into a gray area. Also, other electronic payment providers for the cannabis industry, such as PayQwick, have gotten licensed with full disclosure that they are exclusively serving the cannabis industry.

²²<http://fortune.com/2016/11/18/supreme-court-class-action-lawsuit-atm-fees-visa-mastercard/>

²³<https://www.atmmarketplace.com/articles/scrip-machines-scratch-and-scrape-for-a-piece-of-the-atm-market/>

²⁴<https://www.atmmarketplace.com/blogs/will-cashless-atms-ever-pay-off-for-iads/>

²⁵<https://www.atmmarketplace.com/blogs/will-cashless-atms-ever-pay-off-for-iads/>

²⁶<https://www.law.cornell.edu/uscode/text/18/1960>

The guidance memo issued by the U.S. Department of Justice on February 14, 2014 reiterates that the “provisions of the money laundering statutes remain in effect”²⁷, including the unlicensed money transmitter statute quoted above, while at the same time stating that it will be “using its limited investigative and prosecutorial resources to address the most significant marijuana-related cases in an effective and consistent way... in determining whether to charge individuals or institutions with any of these offenses based on marijuana-related violations of the CSA, prosecutors should apply the eight enforcement priorities described in the August 29 guidance.”²⁸ Thus, one might conclude that the transmission of funds known to be derived from the criminal offense of selling cannabis is only considered as unlawful as the offense of selling cannabis itself.

As a separate issue from the difficulties Cashless ATMs have in operating on US networks in general, where cannabis is concerned, one issue with respect to whether they are compliant with state and federal regulatory frameworks is whether or not they are allowed to use the underlying networks that they are able to operate on. In the case of cash advances from credit cards, the credit card companies’ proprietary networks are used, and as expressed earlier, this constitutes a violation of their rules but is not inherently illegal.

Debit transactions via Cashless ATMs are referred to as “offline debit transactions”, meaning that they do not require a signature and only operate with pin codes. In contrast with online debit transactions, they do not use the proprietary networks established by MasterCard and Visa. Debit transactions are first verified using Electronic Funds Transfer (EFT) networks used for interbank transfers, which include both large regional networks such as Pulse, Star, and NYCE as well as local private networks established by banks. The transactions are later processed, usually at the end of the day, via Automated Clearing House (ACH) EFT networks commonly used for direct depositing and online consumer payments. NACHA, the National Automated Clearing House Association, is the organization that manages the development, administration, and governance of the ACH Network and establishes the roles and responsibilities of operators as well as Originating Depository Financial Institutions (ODFIs) and Receiving Depository Financial Institutions (RDFIs).²⁹ There are two main ACH operators in the US: The Federal Reserve Banks, through the FedACH system, and the Electronic Payments Network (EPN), a private operator.

From a legal perspective, the ACH networks run by the Federal Reserve Banks would have policies and rules that are in line with federal laws and priorities, and therefore transactions involving cannabis would be permitted to the extent that they comply with state regulatory systems, the priorities of the Cole Memo, and the relevant BSA provisions. The Board of Governors of the Federal Reserve System Compliance Guide to Small Entities, Regulation E: Electronic Fund Transfers (12 CFR 205) “provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, point-of-sale (POS) terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs

²⁷<https://www.justice.gov/sites/default/files/usao-wdwa/legacy/2014/02/14/DAG%20Memo%20-%20Guidance%20Regarding%20Marijuana%20Related%20Financial%20Crimes%20%2014%2014%20%282%29.pdf>

²⁸<https://www.justice.gov/sites/default/files/usao-wdwa/legacy/2014/02/14/DAG%20Memo%20-%20Guidance%20Regarding%20Marijuana%20Related%20Financial%20Crimes%20%2014%2014%20%282%29.pdf>

²⁹<https://en.wikipedia.org/wiki/NACHA>, <https://www.nacha.org/news/ach-operations-bulletin-1-2014-questionable-ach-debit-origination-roles-and-responsibilities>

a financial institution either to credit or to debit a consumer's asset account.”³⁰ Under Regulation E there is no mention of any liability for potentially illegal activity conducted through the networks; Section 205.12 states, “... the Federal Reserve Board shall determine whether the request of a state, financial institution, or other interested party is preempted by state laws relating to electronic fund transfers.”³¹

The EPN, which is a smaller operator, would likely follow the same rules established by FedACH and similarly fall under NACHA’s oversight. NACHA’s role in providing guidance appears to focus on providing advice and making requests of its members. For example, in the past there have been instances in which authorities such as the National Association of Attorneys General (NAAG) have asked that members of NACHA refuse to provide electronic payment processing services to entities that appear to support illegal activities such as online tobacco sales³², but NACHA’s involvement appears to be limited to “encouraging the establishment of business practices that ensure that ACH transactions do not facilitate illegal activity.”³³

Therefore it appears that liability for transactions involving an illegal substance or activity falls upon the ODFI and RDFI involved; their subsequent responsibilities with respect to cannabis transactions are laid out in the Cole Memo.

The next question in regard to whether Cashless ATMs constitute a fully compliant solution for the cannabis industry is whether the sale or purchase of cannabis products are concealed or disguised, which would raise the same BSA concerns discussed in relation to merchant services.

In a debit transaction via a Cashless ATM, the transaction is reflected as a cash withdrawal from the consumer’s bank account, and therefore that bank has no means of knowing what the cash is intended to be used for. Similarly, the acquiring (merchant) bank processes the transaction as if cash were received at the cash register, and the merchant’s bank would be well aware that the merchant trades in cannabis, so there is nothing concealed. However, for the purposes of the payment processor and bank that is providing the money transfer services, certain information must be recorded for the transaction in order for it to be processed. This information typically includes a code used to identify the merchant, as well as a Standard Industrial Classification (SIC) code for the business which establishes that it is a dispensary. The precise information will vary depending on the payment processor and underlying bank. However merchant codes are typically not used to identify the product that was purchased as is the case with online debit transactions using MasterCard and Visa’s proprietary networks. As result, there is generally no way of knowing if the product that was purchased was a cannabis product, or an accessory such as a T-shirt.

It is also important to note that even if a product or product category code were included in transactions within a Cashless ATM service, there would be no reason to miscode it as something else, unless the intent was to conceal the nature of the transaction from the card processor or the bank providing the money services. But if this were the case, the SIC code would also have to be misrepresented, as any bank would assume that transactions made at a marijuana dispensary would involve marijuana. Therefore, if the SIC code correctly identifies the type of business, we can conclude that even if there were product information associated with the transaction, said product information would be consistent with the SIC code.

³⁰<https://www.federalreserve.gov/bankinforeg/regecg.htm>

³¹<https://www.federalreserve.gov/bankinforeg/regecg.htm>

³²<https://www.nacha.org/news/use-ach-network-illegal-internet-transactions>

³³<https://www.nacha.org/news/use-ach-network-illegal-internet-transactions>

However, here an implicit assumption is made that the bank providing the money services is fully aware of the nature of these transactions and that the bank does not have an explicit policy against supporting cannabis transactions. Regardless of whether or not a product code is associated with a given sale, Cashless ATM services must comply with the policies and rules established by the bank underwriting the transaction. If the bank has a clear policy of not supporting cannabis purchases, they have the right to terminate Cashless ATM or regular ATM services for violating their policy. Thus it is entirely possible that an unscrupulous Merchant Service Provider or ISO might conceal the fact that the Cashless ATM services they offer involve cannabis transactions, for example by using a different SIC code. In such cases, these services could easily be construed as a breach of the BSA and therefore illegal, as in the case of traditional merchant services. It is equally possible that the bank might frown on such transactions yet not have an explicit policy, or operate on a don't-ask-don't-tell basis, maintaining intentional ignorance on the nature of these transactions. It appears likely that one of these situations occurred in the case of MetaBank, which “discovered” that their ATMs and Cashless ATMs were being placed in dispensaries when the amounts of money they were taking in became too large to ignore, and chose to strictly adhere to federal law.

In the event that Cashless ATM debit transactions involving cannabis purchases do not violate the BSA, and assuming that they do not violate laws regarding the use of federal or proprietary EFT networks, in order to establish their legality and degree of compliance we must still analyze whether any other specific federal priorities outlined in the Cole Memo might be violated. Here again is the list of those priorities:

1. Preventing the distribution of marijuana to minors;
2. Preventing revenue from the sale of marijuana from going to criminal enterprises, games, and cartels;
3. Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
4. Preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
5. Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
6. Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
7. Preventing the growing of marijuana on public lands in the attendant public safety and environmental dangers posed by marijuana production on public lands;
8. Preventing marijuana possession or use on federal property.

None of these priorities would be directly violated by the use of Cashless ATM services. Only Priorities 1, 3, and 6 relate to in-store purchases; Priorities 1 and 6 would be addressed by the workers in the store regardless of how the transaction was structured, and the type of transaction has no bearing on Priority 3. The other priorities are geared towards oversight by financial institutions, as they are in a privileged position to monitor activity over longer periods of time and have a shared obligation under the BSA to know their customers.

FinCEN provides guidance to these institutions by establishing a regime for submitting Suspicious Activity Reports as described earlier. It also provides the list of “red flags” transcribed in the previous section. The type of transaction carried out is irrelevant to nearly all of these red flags, meaning that whether the transaction was in cash, or via Cashless ATMs, or any other means of electronic payment processing, has no bearing on the red flag. However, there is one that is relevant to our analysis:

“A marijuana-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or

large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.”

Therefore, if a payment processing company or bank providing the money transmission services for Cashless ATM system is located outside the state where the terminal is located, this could violate one of the priorities of the Cole Memo. Note that this does not make the Cashless ATM illegal, it simply requires a Marijuana Priority SAR to be filed by both the bank providing the money services and the receiving (merchant) bank. Whether or not this would lead to federal prosecution is unknown; the Cole Memo seems to suggest that the simple transfer of funds would not warrant prosecution. Nevertheless, an investigation of repeated interstate transfers to a dispensary could cause banks to review and possibly change their policies regarding cannabis.

It can therefore be concluded that Cashless ATMs in principle offer a compliant solution to the cannabis industry. However, the MSP must be a licensed money transmitter in the state of operation, and the payment processor and bank it uses to perform the transfer should ideally be located in the same state in order to avoid any potential federal investigations. It should also not make any attempt to change or misrepresent the information that is associated with a given transaction when it is sent to the payment processor and the bank providing the money services. If these conditions are met, then there is no reason to believe that Cashless ATMs cannot be considered a fully compliant solution.

Unfortunately, the reality is that, aside from the network issues that Cashless ATMs have, nearly all the banks and credit unions that are active supporters of the cannabis industry are currently too small to take on the business of a payment processing company. As result, electronic payment processors have to appeal to large national banks that are much less likely to do business with the cannabis industry.³⁴ This creates an environment that can foster deception. Additionally, larger banks with diverse activities are prone to changing their policies suddenly if cannabis operations that they support reach a level significant enough to prompt federal scrutiny, leading to terminated services. And of course the payment processors and banks that provide the underlying money services are often located in other states. As result, despite the fact that Cashless ATMs may in principle be a compliant solution to the cannabis industry’s need for handling electronic payments, in practice they may not be suitable solution. Financial institutions and cannabis businesses that seek to use Cashless ATMs should carefully vet the specific services provided by an MSP to ensure compliance.

Closed-loop services

Electronic payment processing services are also provided to the cannabis industry via so-called “closed-loop services”. Closed-loop refers to the fact that for any given transaction, the issuing bank, the acquiring bank, and the payment processing company are all connected via EFT (typically ACH) or private networks and are not reliant on MasterCard or Visa’s proprietary networks or subject to their rules and restrictions. Paypal, Google Wallet, and Apple Wallet are examples of a closed-loop system that do not participate in the cannabis industry. PayQuick and CanPay are two examples of closed-loop systems built specifically to facilitate cannabis purchases.

Closed-loop systems have some clear advantages over other electronic payment processing solutions. First, the systems are easier to set up so that all participants are located within the same state in order to avoid potential prosecution for interstate transfers of proceeds from cannabis transactions as discussed in the previous section. Also, there is explicit “buy-in” by all the participants, who are well aware that

³⁴<http://www.cannalawblog.com/marijuana-payment-processing/>

transactions involve cannabis as well as the regulations and risks involved. This effectively eliminates the problem of miscoding found in traditional merchant services, since participants have no reason to conceal or hide the nature of their transactions. Finally, closed-loop systems generally require merchants to open merchant accounts with the same financial institution where they have their own merchant accounts, so that a high percentage of transactions occur between accounts managed by the same bank. This allows for a higher degree of oversight by the bank, since (in many cases) they know the customers on both sides of the transaction.

Given that closed-loop payment processing services can be set up not to conduct transactions that cross state lines, do not conceal the fact that they are facilitating cannabis purchases, and do not use any proprietary networks, they avoid many of the compliance concerns presented by traditional merchant services and Cashless ATMs.

Closed-loop services typically force users to open accounts with them prior to making any purchases. During this process, the payment processing company has an opportunity to fulfill “know your customer” requirements and vet users to the extent required by the Cole Memo and subsequent FinCEN guidelines. Note that for cannabis businesses operating on a cash-only basis, purchases can be completely anonymous. In contrast, on closed-loop systems all users are registered with the payment processor and must supply identifying information and bank checking account information. From a compliance point of view, this is far preferable as it provides the payment processors and banks the means to monitor purchasing patterns over time for any given client.

There are different implementations of closed-loop payment processing services. For the purposes of this paper, we examine and compare the approaches taken by two competing companies: CanPay and PayQwick.

CanPay employs a simple and straightforward approach, based entirely on offline debit card transactions without supporting credit cards. CanPay’s “accounts” are not really accounts in a traditional sense, meaning that its clients do not deposit funds in advance and leave a balance that could be applied towards purchases. Rather, it uses its accounts as temporary repositories to deposit money debited from purchasers’ checking accounts and transfer the same money to merchants’ accounts at the time of making a purchase.

Payments are made through a smartphone app, where users enter in the amount of money for a payment and a temporary 2D barcode containing the relevant information for the transaction is displayed on a phone which can be scanned at a cash register to complete the purchase. If not scanned within 30 minutes, the transaction is cancelled.

The important feature of all closed-loop systems with respect to the cannabis industry is that because debit or credit transactions are only used to credit an account on the system and not make actual purchases, they bypass MasterCard or Visa’s anti-cannabis policies and relieve the issuing banks from any liability that might be associated with a cannabis purchase. On the other end of the transaction, CanPay forces merchants to open accounts with a financial institutions that agree to participate in their closed-loop system and with which CanPay has its own merchant account. Funds can be easily transferred from CanPay’s merchant account – which holds all the funds involved in all the transfers occurring at any given time – into the cannabis merchant’s account at the same bank.

Because CanPay does not hold onto the money but simply serves as a conduit for transferring money from one bank account to another using ACH networks, it leaves the issue of handling state compliance

to the merchant, who rings up the sale on a POS system that is integrated with a state compliance system such as Metrc or Biotrack. Federal compliance is left to the receiving bank, who must submit the federal SAR reports upon the receipt of the money into CanPay's merchant account, or after it is transferred to the merchant's account, or both depending on how it interprets FinCEN's guidelines. From the receiving bank's point of view, cannabis transactions that occur via CanPay's system are treated similarly to electronic payments made for non-cannabis (i.e., legally sellable) products. This is preferable to cash transactions for banks for two reasons: first, cannabis purchasers are not anonymous and their purchasing patterns can be monitored; and second, it reduces the amount of cash that banks have to deal with, which entails additional bureaucracy and security risks.

PayQwick has a slightly different implementation, which in some ways is more traditional and similar to familiar products like PayPal. It provides a system whereby users debit their checking accounts and transfer funds into their PayQwick accounts prior to making purchases. Users can then make payments out of these accounts when purchasing items, either online or in-store. PayQwick offers its own card, which can be swiped at its terminals to make payments, and has additionally implemented a new service that allows users to swipe their debit and credit cards where payment is made from their PayQwick account instead of directly via the card. In these cases, a purchaser enters in the amount of a sale, swipes their credit or debit card, and funds are transferred out of their PayQwick accounts and into the merchant's PayQwick account. PayQwick also allows users to open temporary accounts on the spot if they have not previously set up a PayQwick account. In such cases, when purchasers swipe their cards, money is debited from their checking account and placed into a temporary PayQwick account created for new users using the identification information read from the card. Payment is made to the merchant out of this temporary account, and the purchaser is sent an email requesting them to register their account information later.

An attractive feature of this implementation is that if a PayQwick account holder makes a purchase that costs more than the balance of their account, the additional funds necessary to cover the cost of the purchase are automatically transferred into their PayQwick account from their checking account via an ACH request. As a result, the balance that PayQwick account holders maintain in their accounts is essentially meaningless; they could credit their accounts with a very small amount of money and simply channel funds from their checking account to the merchant's account on demand, with the PayQwick account simply acting as a temporary repository through which money is transferred in order to avoid infringement of MasterCard and Visa's anti-cannabis policies. This is similar to the CanPay model, but with one important difference: the funds are not immediately transferred to the cannabis merchant's bank account, but remain in the merchant's PayQwick account. The decision of when and how much money to transfer from a merchant's PayQwick account to a merchant's own account with the bank is left up to the merchant, as with PayPal.

Note that the money exchanged between all participants in this closed-loop system is aggregated into a single PayQwick merchant account. An interesting result of this arrangement is that if a retailer purchases \$1000 dollars of marijuana from a wholesaler by transferring money from the former's PayQwick account to the latter's PayQwick account, no money is actually moved. PayQwick simply records the transfer in its own books, leaving all the money in its merchant account untouched.

Because (at the time of writing) PayQwick appears not complete transactions by depositing funds from purchases into separate merchant accounts, and instead retains the money in its own account at the bank, the bank may be in a poor position to handle compliance with state and federal regulatory systems. It doesn't know when individual purchases are made or what the amounts are; PayQwick essentially represents a black box from which amounts of money are occasionally transferred into other accounts in a

manner completely disassociated from individual purchases. Therefore, PayQwick handles compliance, both by integrating with state tracking systems such as Metrc and Biotrack and filing the appropriate SAR reports pursuant to the Cole Memo and FinCEN's guidelines. The bank also has to file the relevant SAR reports when funds are moved from PayQwick's account to a merchant's account, but since these funds have been disassociated from any actual purchases, the bank's workload is greatly reduced. If, for example, a dispensary client makes 750 sale transactions totaling \$50,000 over a month and then transfers the money as a lump sum into the dispensary's merchant account at the end of the month, the bank would file a single SAR report based on the dispensary's proceeds for the month. In contrast, under other closed-loop systems such as CanPay's, the bank would have to file 750 SAR reports, one for each individual transaction. This obviously saves the bank a lot of effort.

In terms of legality, there is little evidence that these kinds of closed-loop payment processing services are doing anything that could be characterized as illegal. However, we should analyze carefully whether these systems could present any concerns with respect to federal compliance.

First, it should be pointed out that although closed-loop systems don't technically violate MasterCard and Visa's policies regarding cannabis transactions, in the sense that no purchases of these products are ever recorded on their systems, there is nothing preventing these credit card companies from refusing to allow their cards to be used by cannabis-specific closed-loop payment processors. Companies like PayQwick and CanPay are both clear about their intentions to serve the cannabis industry and credit card companies have the right to deny them service. However, in the alternate scenario discussed earlier where their cards are being used directly for cannabis purchases under traditional merchant services, they cannot overlook the fact that their rules are being flagrantly violated and that substitute merchant codes are being used. If MasterCard or Visa have sufficient reason to be suspicious, they could be prosecuted under federal law for aiding and abetting the *concealment* of a cannabis transaction, which is illegal under the BSA. However under the closed-loop scenario, they have additional protection from this liability by the intermediate step of transferring funds into a separate account, which ensures that all their records remain "clean". Under this scenario, they could only be prosecuted for aiding and abetting the *purchase* of cannabis, which the Cole Memo has essentially reduced to a lawful and highly regulated activity that is not a priority in terms of prosecution. Therefore, MasterCard and Visa are probably unlikely to refuse service to these closed-loop payment processors.

In terms of how federal compliance is handled by the payment processing companies themselves, we need to examine two issues: first, to what extent do they impact the due diligence that financial institutions must undertake for their cannabis clients, and second, the issue of when and how SAR reports are required to be filed.

FinCEN's due diligence guidelines are stated as follows:

"In assessing the risk of providing services to a marijuana-related business, a financial institution should conduct customer due diligence that includes: (i) verifying with the appropriate state authorities whether the business is duly licensed and registered; (ii) reviewing the license application (and related documentation) submitted by the business for obtaining a state license to operate its marijuana-related business; (iii) requesting from state licensing and enforcement authorities available information about the business and related parties; (iv) developing an understanding of the normal and expected activity for the business, including the types of products to be sold and the type of customers to be served (e.g., medical versus recreational customers); (v) ongoing monitoring of publicly available sources for adverse information about the business and related parties; (vi)

ongoing monitoring for suspicious activity, including for any of the red flags described in this guidance; and (vii) refreshing information obtained as part of customer due diligence on a periodic basis and commensurate with the risk. With respect to information regarding state licensure obtained in connection with such customer due diligence, a financial institution may reasonably rely on the accuracy of information provided by state licensing authorities, where states make such information available.”³⁵

Most of these tasks have to do with “knowing your customer” and are conducted by the bank when individual merchants open accounts, and are not impacted by what kind of payment processor is used for making electronic payments. The only one that is relevant is “ongoing monitoring for suspicious activity, including for any of the red flags described in this guidance”; in other words, the filing of SAR reports.

CanPay does not file SAR reports, and leaves this responsibility up to the bank. However, due to the nature of their implementation the funds are first transferred into their account, and subsequently into the merchant’s account as a separate transfer. Would the bank have to file two separate SAR reports for the same transaction, to reflect its division into two distinct operations? Presumably not, as the reports would be identical and there would be no benefit to FinCEN in terms of additional information that would be helpful in identifying whether any of the Cole Memo priorities had been violated.

In the case of PayQwick, as noted earlier, transactions would seem to only take place in their own books. All PayQwick transactions take place between two parties who each have PayQwick accounts. The funds are only segregated on PayQwicks books, from the point of view of the bank, all the actual funds are located in PayQwick’s single merchant account with the bank. Therefore, when a transaction occurs, PayQwick moves a number from one column to another, but nothing happens to the funds in the bank. The bank would be unaware that any transactions took place. Whether or not PayQwick decided to file a SAR report or not would be up to them; no one outside the company would know if they did or didn’t.

In the case that PayQwick decided to take the point of view that the Cole Memo did not require them to file the SAR reports if no money moved from one bank account to another, this would easily produce a situation in which the number of SAR reports from a given state would decline rapidly. This would no doubt provoke the DOJ to intervene, under the assumption that transactions were being “concealed” from them. It would be hard to imagine that they would not perceive this as a violation of the Cole Memo. Similarly, very few banks would be comfortable with this arrangement, as they could also be implicated in any subsequent investigation.

To be safe and ensure full compliance with the DOJ guidelines, PayQwick would probably have to diligently file SAR reports with every transaction, even though no money appears to change hands in the bank. This would be easy enough to do, and in turn, most banks would be likely to consider PayQwick an attractive option, as it would shift a lot of the burden of filing the SAR reports. Also, the filing of the SAR reports would likely have to be monitored by the bank in order for it to adequately fulfill its know-your-customer requirements under the BSA.

In conclusion, in the cannabis industry today, closed-loop solutions such as PayQwick and CanPay would seem to be not only fully compliant and legal solutions, but also the solutions that are most appropriate for cannabis businesses due to their comparative stability and efforts made to partner with specific financial institutions.

³⁵<https://www.fincen.gov/resources/statutes-regulations/guidance/bsa-expectations-regarding-marijuana-related-businesses>