White Label ATM Sector in Canada

Background

In Canada, the major financial institutions have their own bank-owned and branded ATMs. After a Competition Bureau decision in 1996, independent operators (known as acquirers and independent service operators) were allowed to operate ATMs and be part of the Interac network. "White label" or private ATMs provide cash dispensing services by linking to financial institutions with the Interac and VISA and Mastercard networks. They are usually located in non-traditional places, such as bars, stores and restaurants. The sector's business model is complex given the different players involved (e.g., network connectors, ATM sellers, and owners) and is integrated with other sectors, such as financial institutions, payment network providers, armoured car services, and equipment manufacturing businesses.

Any individual can own or operate a white label ATM (WLATM). According to the Canadian Bankers Association, there are approximately 51,000 WLATMs in Canada. Currently, none of the parties involved in the WLATM industry are subject to the *Proceeds of Crime (Money laundering) and Terrorist Financing Act* (PCMLTFA) nor addressed in the Financial Action Task Force (FATF) Recommendations. However, Quebec does have legislative requirements with respect to WLATMs. This legislation is intended to deter their use by money launderers and limit opportunities for tax evasion.

Certain aspects of the industry are also regulated by the following codes and standards:

- The Standards Council of Canada (SCC) has a voluntary code of standards for ATMs. This code covers the construction and security performance of ATMs and seeks to provide protection against the unauthorized removal of currency.
- The Office of Consumer Affairs (OCA) has a voluntary code of practice for consumer debit card services, prepared by the Electronic Funds Transfer Working Group. It outlines industry practices as well as consumer and industry responsibilities and serves to protect consumers in their use of debit card services in Canada.
- Rule E1 of the Canadian Payments Association (CPA) covers the obligations of a Delivering Direct Clearer (DDC). This rule ensures that information protection and verification requirements are met during the encryption and decryption of the secret code (PIN).
- The Interac Association has operating regulations which govern, for example, record keeping, due diligence and related requirements, which were developed primarily to mitigate the risks associated with debit card fraud.

These codes, regulations and standards are in place to ensure that consumers are protected during their use of debit services and that the settlement process is managed appropriately.

Interac

Interac is the organization responsible for the development and operation of a national network of two shared electronic financial services: Shared Cash Dispensing at automated teller machines (ATMs) and Interac Direct Payment (IDP), Canada's national debit service. The Interac Association defines itself as "a national organization linking enterprises that have proprietary

networks so that they may communicate with each other for the purpose of exchanging electronic financial transactions."

Within the Interac Association, there are two types of members: direct connectors and indirect connectors. The first type can be defined as a member who "connects directly to the Shared Cash Dispensing Service or Interac Direct Payment service through the Inter-Member Network." In simple terms, the direct connectors are almost all "deposit taking" financial institutions. Under Interac Association's decentralized network structure, each Direct Connector must maintain a physical link to all Direct Connectors in the network.

The second type of members is the ones who access the Inter-Member Network by connecting through a Direct Connector. WLATMs are connected to the Interac Inter-Member Network through an Acquirer (third party processor and/or indirect connector) and a financial institution (direct connector or connection service provider). The Acquirer would be the one who holds the information with regards to the location and the ownership of the machine.

Interac also operates as a self-regulatory body for the ATM industry and imposes various operating and security rules on its members. Interac's current rules require members to be prudent and address potential risks to themselves and the network. Specifically, Interac members are required to conduct a minimum level of due diligence on their business partners that includes ensuring that the partner can comply with Interac's rules. For new business partners that have operated for fewer than two years, additional CDD measures are required, including corporate ID verification, corporate credit checks and limited criminal record checks for directors and owners. Interac's new rules require Members (i.e., Acquirers) to perform customer due diligence on ATM cash owners and collect information on the ATM's source of funds, including a criminal background check . These rules also include a formal document review process that requires all Members to hire an auditor to ensure that all of the required documents have been collected and retained for each ATM. Findings of non-compliance with the AML rules have prescribed time periods for remediation and could result in disconnection of the ATM from the Interac network. To date no one has been denied access to the Interac network or has been removed from the Interac network for AML reasons.

In combination with these rules, a "Security Unit" was to be implemented within Interac to enhance the flow of information between Interac and law enforcement. This would provide a point of contact for law enforcement to assist them with their investigations.

Observed Money Laundering/Terrorist Financing Methods

R13 Statutory Limitations on Disclosure

[redacted]

1. A white label ATM operator can hire an ATM Service Company to load cash in the ATM, which, unbeknownst to the WLATM operator, is criminally owned, and places dirty cash into the WLATM. Alternatively, cash may be purchased from another company, which, again

unbeknownst to the purchaser, is criminally owned and provides dirty cash to the ATM owner, who then places the cash into the ATM.

2. The placement of dirty money into a WLATM by a business owner involved in criminal activity, or with connections to organized crime[1]. In a 2013 news article, a retired RCMP officer described how an organized crime group could arrange to have an ATM placed in a club and launder money[2]. The owner of the club — a front person chosen for their lack of criminal record — would apply for the necessary security clearance and, after receiving it, could stock the machine with a mix of bar sales and drug proceeds. As long as the machine stayed under a safe limit, such as $5,000 a day, it would be unlikely to draw attention. There are no hard statistics for how often this might be happening, but the 2008 RCMP Strategic Intelligence Assessment – Project SCOT report estimates Hells Angels bikers control at least five per cent of the private ATM business in Canada. The same report says at least $315 million a year could be laundered through WLATMs, and could easily reach to $1 billion. In 2014, Winnipeg organized crime rings took dirty money and "cleaned it" through the use of the ATM, legitimizing it as the money returned by financial institutions. In 2014, six Winnipeg ATMs were seized from four bars in an organized crime raid.
3. The creation of a company, purportedly involved in the ownership/operation of WLATMs, can be used as a cover for criminal activities including money laundering since the operation of white label ATMs is a cash-intensive business. According to the 2007 FINTRAC report[3], one feature that makes WLATMs particularly vulnerable to money laundering is the fact that operators can remain virtually anonymous while conducting their activities. This is mainly due to the number of tiers in the ATM ownership hierarchy. As WLATMs are sold and re-sold to different parties, the change in ownership is not always reported to the upper tiers of the hierarchy.

As such, there are principal money-laundering vulnerabilities with these machines. Operators can load cash in the WLATMs themselves, using cash obtained from a number of sources including cash registers, armoured car services, or other private cash providers. Operators can also hire a third party to service an ATM and ensure that there is always cash loaded into the machine. It is possible that a cash provider could launder money through an ATM by loading dirty money into the machine without the operator's knowledge. Moreover, an operator can commingle cash from several sources, making it virtually impossible to trace the origins of the cash. This provides criminals an opportunity to place dirty cash into the economy, laundering it through withdrawals made by customers using the ATM.

Furthermore, the ownership structure of the WLATM industry is such that an owner/operator may be able to operate an ATM without the Interac Association's knowledge. The hierarchical structure of the industry relies on direct and indirect connectors to connect ATMs to the network. Each machine is not typically operated by the Interac member that provides the connection to the network. Independent Sales Operators operate the machines, or sell and lease them to other businesses or individuals to operate. Interac maintains a list of each individual ATM, but they may not have all the necessary detailed information on the operation of the machine.

Conclusion

The money laundering vulnerability does not lie with the clients withdrawing funds from the WLATMs. Authorized third parties, independent of the ATM cash owner, record and retain information about every dollar that passes through a WLATM in Canada. The information recorded by third parties includes a transaction record number, the amount withdrawn, the date and time of the withdrawal and the Canadian bank account to which the funds withdrawn are electronically settled. There are no WLATM withdrawals

[1] https://www.cbc.ca/news/canada/manitoba/no-name-atms-a-tool-for-money-launderers-rcmp-say-1.2538162
[2] https://www.cbc.ca/news/canada/private-atms-vulnerable-to-money-laundering-1.2288659
[3] https://archive.org/details/813221-2007-fintrac-report-on-white-label-atms/page/n11

and settlements of any amount, at any time, that are anonymous. Independent third parties clearly record and retain the details of the money flow. The WLATM vulnerability lies in the loading of the machines, which can be done anonymously. Companies owning and loading WLATMs for themselves or other legitimate businesses may be criminally controlled. Criminals can offer ATM services within different legitimate businesses or set them up in their own businesses, and load those ATMs with illicit cash.

The unregulated nature of the industry leads to several money laundering vulnerabilities, which are omnipresent regardless of whether the owner/operator is a witting or unwitting participant. This lack of oversight can provide organized crime a favourable environment to use ATMs to conduct various illegal activities, including money laundering, fraud and distribution of counterfeit money[4].

[4] https://vancouversun.com/news/crime/police-in-canada-not-following-the-money-of-crime-groups-international-report-says