Anti-Money Laundering & Third-Party Payment Processors

AML / CTF OVERSIGHT

Marcia Francis, CPA, CGA, CFE, CAMS-Audit

2019
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

Table of Contents
Introduction............................................................................................................................. 2
  Current Problem .................................................................................................................. 2
  Audience ............................................................................................................................ 2
  Key Terms .......................................................................................................................... 2
Background .......................................................................................................................... 3
Current Controls of TPPPs Money-Laundering Risk ............................................................. 6
  Role of Payment Card Networks ....................................................................................... 8
  Collaboration Is Key .......................................................................................................... 8
  Private Label ATM Due-Diligence Overview .................................................................... 9
  Merchant Due-Diligence Overview .................................................................................. 11
  Money Laundering Goes Digital....................................................................................... 11
TPPP Management Oversight Program ............................................................................... 13
  Third-Party Payment Processor’s Risk-Based Assurance ................................................. 15
  Case Study ....................................................................................................................... 16
Conclusion ............................................................................................................................ 17
References ............................................................................................................................ 18
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

Introduction

Third-party payment processors (TPPPs) are critical participants in the payment ecosystem. TPPPs are legally responsible for the funds of each electronic transaction when those funds are not in the hands of either the buyer or merchant. This paper will focus on the facilitation of payments between buyers and sellers, and how they can work collaboratively to reduce money-laundering risk.

Current Problem

The prevailing argument is that the inclusion of third-party payment processors in the payment ecosystem adds complexity and increases the financial institutions’ exposure to money-laundering and terrorism-financing risk.

Audience

This paper is intended to provide information for acquiring financial institutions, payment card network operators (PCNOs, card networks), payment vendors, third-party payment processors (TPPPs, payment processors), payment gateways, independent sales organizations (ISOs), and merchants. It will also be of use to anti-money laundering and counter-terrorism financing (AML/CTF) regulators and professionals.

Key Terms

Third-Party Service Provider (TPSP)
A TPSP, also known as a payment service provider is a non-bank payment vendor that connects merchants, consumers, card networks, and financial institutions to the electronic financial system to accept card-present and card-not-present payment transactions. The financial transactions they support may be:

- initiated by an in-store credit card, debit card, or prepaid card accepted on a payment terminal by means of contact or contactless technology,
- mobile-device-based contactless transactions using NFC or QR code technology at a payment terminal, or
- online financial transactions initiated at a computer on the Internet.

TPSP’s can also be payment service providers that function exclusively in a business-to-business environment between merchants, card networks, and acquiring financial institutions. These payment service providers do not access a consumer’s financial institution account information.

Third-Party Payment Processor (TPPP)
A TPPP, also known as a payment processor, is a customer of a financial institution. The payment processor uses the financial institution’s electronic transfer services to process payments on behalf of others. They accept and process card payments on behalf of a merchant, an ATM cash owner, or an ATM operator, resulting in a transfer of funds to the merchant or ATM owner or ATM operator.

Money-Laundering Risk
This is the possibility that an organization in the payment ecosystem may be used to help launder (or conceal the illicit source of) money and, thereby, put itself in a position of legal exposure. More specifically, it is the possibility that the organization could accept funds derived from the proceeds of crime, fraud, and other illegal activities.
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

Background

Card payments are financial instruments used to transfer value in the form of money. They are an essential part of each country’s economy and are usually performed for the provision of goods or services. The transfer values are typically stored in depository accounts at financial institutions, such as banks, credit unions, and so forth. Card-payment participants, consumers, and processors use multiple channels to make payments. These payment channels include card-present (or in-person) payments, card-not-present (or online) payments, mobile application payments, and other payment alternatives. Each can have different operating characteristics, rules, and settlement mechanisms.

This paper is designed to offer practical knowledge for those who operate in the payment ecosystem as TPPPs by outlining how regulatory guidance can lessen the challenges faced by these organizations, and also allow them to demonstrate that there is appropriate AML/CTF oversight in place.

Card payments will continue to grow globally and so will the risks. This growth increases the need for education, diligence, process controls, and tools to reduce legal and financial exposure for participants in the system. In 2017 alone, payment card volume hit $20.020 trillion with projections of general branded card volumes to grow to $78.453 trillion in the next ten years.

1 See FDIC guidance and other information on Third-Party Payment Processors:
Delivering the above volume requires coordinated efforts of four main participants in each debit and credit card transaction, whether it is in person or online. Let’s explore each participant:

1. **Acquirer or Acquiring Financial Institution** – This entity is responsible for ensuring that monies are transferred correctly and applied accurately. This entity may be a financial institution, a credit union, or a payment processor.

2. **Payment Card Network Operator (PCNO/card network)** – This entity is responsible for handling and monitoring all transactions in the card network. The global payment card networks are American Express, Discover/Diners Club, JCB, MasterCard, UnionPay, and Visa. These card networks handle the worldwide processing of debit and credit card transactions, acting as proxies between consumers and merchants. Each card network settles the net amount of the day’s card transactions between all of its member financial institutions using payment systems such as Canada’s Automated Clearing Settlement System (ACSS) or the U.S. Automatic Clearing House (ACH).

3. **Issuer or Issuing Financial Institution** – This entity is responsible for issuing debit, credit, and prepaid cards to their customers. They are responsible for charging their cardholder’s account for the cost of the goods or services purchased.

4. **Payment Gateway** – This entity performs online sales, which are essentially any payment method other than cash and cheque. They are the middleware that convey these card-not-present (CNP) transactions between a merchant’s website and the payment processor.
A payment processor is a client of a financial institution. It processes payments on behalf of others, which may include merchants, ATM cash owners and ATM operators using the financial institution’s electronic funds transfer (EFT) services. In order to accept card payments, disburse funds, and meet compliance needs all those entities must purchase services from the payment processor.

The payment processor’s financial institution does not have contractual relationships with the payment processor’s customers. Even so, the financial institution’s electronic funds transfer services are used to move money from the payment processor’s account to their customers’ accounts. The customer accounts may be located at other financial institutions; so, in order to protect the relationship between financial institutions, the payment processor must exercise due diligence in knowing their customers, merchants, ATM owners, and ATM operators.

Diligence may be simpler when the payment processor and its customers’ accounts are at the same financial institution. In such cases, the financial institution would have independently performed its own consistent onboarding, due diligence and ongoing due diligence over all these accounts.

It should be noted that although the payment processor’s customers may not be customers of the payment processor’s financial institution, the financial institution is the ultimate owner of any relationship that the payment processor creates, and, as the gatekeeper of the payment system, the financial institution is responsible for all payments processed. The financial institution contractually passes on compliance and know-your-customer (KYC) functions to the payment processor. Even then the financial institution must monitor and ensure that the payment processor performs the necessary compliance functions as the financial institution would do with its direct customers.

The payment ecosystem is built on relationships. The importance of third-party relationship in the payment ecosystem is entrenched as consumers’ card-payment use increases. These relationships are formed to satisfy and exceed ever-growing merchant and consumer desires to have better payment products and services. Therefore, payment processors are motivated to establish relationships with other third parties, such as independent sales organizations (ISOs) that take on the work of dealing directly with merchants and managing aspects of merchant risk. This allows payment processors to focus on their core processing business and still grow their portfolio. Even though the payments industry has had a solid foundation of collaboration and information sharing for many years, maintaining and demonstrating AML/CTF compliance to financial institutions remains critical for business stability and continuity.

AML/CTF regulators and governments are aware that payments are becoming faster, frictionless, and cheaper, hence, the increased scrutiny over these activities and over payment processors. Financial institutions with payment processor customers must demonstrate compliance with both government AML/CTF regulations and card network rules. Both sets of rules and regulations are in place to ensure financial institutions have active compliance programs that are
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

operational and effective to prevent its products and services from being used for illicit purposes. As gatekeepers of the payment system, financial institutions need to have full confidence in their relationship with customers, and that starts with documented and complete understanding of their payment processor customers and their third-party business operations. KYC and due diligence form the basis of those relationships. The financial institutions must ensure that they clearly communicate all AML/CTF policies and procedures to their payment processors. The payment processors and their third-party operators, in turn, must ensure the financial institutions’ AML/CTF policies, procedures, and reporting requirements are fulfilled to avoid any significant challenges with anti-money laundering (AML) sanctions and regulations.

Current Controls of TPPPs Money-Laundering Risk

The current AML/CTF oversight of payment systems is based in part on an institutional approach where certain organizations, such as financial institutions, money service businesses, and casinos are subject to AML/CTF regulations, while others are not regulated. The United States’ Bank Secrecy Act (BSA) and Canada’s Proceeds of Crime (Money Laundering) and Terrorist Financing Act require financial institutions to assist their governments in detecting and preventing money laundering. The AML/CTF regulations define “financial institution” as including banks and other traditional financial companies, as well as money service businesses (MSBs) and other non-bank entities. A money service business is an all-encompassing term that covers money transmitters, currency dealers, check cashers, and other similar service providers.

Many countries have acts like the United States’ BSA and Canada’s Proceeds of Crime (Money Laundering) and Terrorist Financing Act that require banks and other financial institutions to:

- establish and implement an adequate AML program;
- conduct required due diligence on their customers, including TPPPs; and
- detect and report suspicious activities.

Traditionally, payment processors are not regulated. However, in the United States, payment processors who are money transmitters fall within the BSA/AML regime, which means they are regulated. They are designated AML/CTF reporting entities and must comply with AML/CTF regulations.

Definition of Money Transmitter

The definition of *money transmitter* for the purpose of BSA regulations, found at 31 CFR 103.11, includes:

A. any person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds dominated in currency, and transmits the currency or funds or the value of the currency or funds by any means through a financial agency or institution, a Federal Reserve Bank, or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both or an electronic funds transfer network; or

B. any other person engaged as a business in the transfer of funds.
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

In some cases, payment processors who are money transmitters can be excluded from money service business AML/CTF requirements if they pass FinCEN’s four-part test to qualify for an exemption to the money transmitter definition. They are then required to be compliant with the AML/CTF requirements of their financial institution.

**FinCEN Payment Processor Exemption**

FinCEN stipulates four conditions for the payment processor exemption to apply to a particular business pattern.

1. The entity providing the service must facilitate the purchase of goods or services or the payment of bills for goods or services (other than money transmission itself).
2. The entity must operate through clearance and settlement systems that admit only BSA-regulated financial institutions.
3. The entity must provide the service pursuant to a formal agreement.
4. The entity’s agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds.

The financial institution’s payment processor customers who are exempt from AML/CTF are typically considered high-risk because they process payments for other parties that are themselves not subject to AML/CTF requirements. The risk is heightened because money is in constant flow for a payment processor. That is, the funds are continually passing from one source to the next and, if not carefully managed, could expose the financial institution and the payment gateway to financial and money-laundering risks.

In the absence of a payment processor specific regulatory framework, the onus is on the financial institutions to ensure they have robust KYC processes when establishing these relationships. That is, the underwriters must evaluate payment processor applications and determine whether the risk, profit, and potential business relationship justify approval for that payment processor to become a customer of the financial institution. The approval process is crucial and requires a high level of vigilance to ensure that payment processors will adhere to the specific rules outlined in the contract and procedural documentation. Financial institutions must ensure funds that flow into and out of the account are in line with the information provided by the payment processor, hence, the need to establish proper processes and controls while implementing rigorous review for high-risk relationships.

Banks must:
- create policies and procedures to govern the relationship and ensure compliance with AML/CTF and KYC requirements,
- implement detailed policies for approval of new TPPPs,
- understand TPPPs services,
- know TPPPs customer base, and
- know the identity of the ultimate beneficial owner of the account.

---

Role of Payment Card Networks

Card networks are important participants of the payments ecosystem. The card schemes’ operating regulations stipulate who can connect to the card networks, their roles, and responsibilities. The major card network operators, such as American Express, Discover/Diners Club, JCB, MasterCard, UnionPay, and Visa, maintain an anti-money laundering/counter-terrorism financing (AML/CTF) program. It is a critical component of members’ underwriting and due-diligence process. All members must complete the AML/CTF questionnaire and certification, and provide ownership and beneficial ownership information where applicable.

In Canada, only federally regulated financial institutions may perform card network payment services, such as transferring funds to merchants' account. Typically, federally regulated acquiring financial institutions do not process merchants' payments directly to the merchant, but instead outsource the payment processing function to a third-party service provider, the payment processor.

Financial institutions and their payment processor customers are required to comply with the card network rules and regulations. The rules and regulations define the level of due diligence the acquiring financial institution must perform to ensure the payment processor is eligible to participate in payment activities. The due-diligence guidelines for payment processors are:

- the validation of ownership and business license;
- the evaluation of financial status;
- background, credit, criminal, company checks, and so forth;
- adequate insurance coverage; and
- the review of business strategy or business plan.

As the acquiring financial institution and card network member, the institution must register an approved payment processor with the card network before payment services start. Similar to the financial institutions’ AML/CTF compliance, the card networks are ultimately responsible for all payments processed from their acquiring financial institution clients. Once again, the card networks are the gatekeepers of the payment system.

Collaboration Is Key

Cooperation between the payment processor and its financial institution is paramount. The financial institution needs to know the beneficial owner of the relationship is legitimate and is not conducting any activity that would violate AML/CTF or sanctions rules. Therefore, the payment processor must be transparent and provide all requisite information for the financial institution to understand the payment processor’s business model, allowing the financial institution to complete its own KYC due diligence. For payment processors with third-party relationships, they must ensure they have documented third-party risk-management policies, regular risk assessments, perform their due diligence, and ensure procedures are aligned with the financial institution’s requirements. These controls must also be monitored and tested for effectiveness.

Required Documentation

- Policies, standards and procedures that identify the level of due diligence required for new and existing merchants, ATM owners, and ISOs
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

- Third-party relationship agreements that identify the roles and functions performed by each
- Sample agreements that include a termination clause
- A list of new merchants and ATM owners—must be maintained and communicated regularly to the financial institution
- A list of new third-parties—again, must be maintained and communicated regularly to the financial institution
- Review records ensuring that all third-parties promotional material, including websites, have been reviewed for compliance with business rules
- Monitoring reports on merchants for chargebacks, refunds, unauthorized returns, and other return thresholds, as well as spikes in request of proof of authorization and any other suspicious activity

There is a significant amount of collaboration and exchange of relevant data between all payment participants and governments to deter bad actors from entering the ecosystem. They do get in occasionally, fraudulently, as they do not play by the same rules.

For example, PacNet, an international payment processor and money-services business based in Canada, helped fraudsters gain access to U.S. financial institutions by knowingly processing payments on behalf of mail-fraud schemes. PacNet used its relationships with banks to set up accounts for customers who committed mail fraud. These customers’ mail-fraud cheques were sent to PacNet and deposited into its account. PacNet would withhold its commission and transfer the remainder to the bank accounts of its mail-fraud customers. A defrauded customer’s paid/cancelled cheque would typically have PacNet name stamped on the back of the cheque. Its operations were eventually shut down by the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC), and PacNet is now designated as a significant transnational criminal organization (TCO). (A transnational criminal organization is an organization identified by the United States that threatens U.S. national security and/or foreign policy.)

Private Label ATM Due-Diligence Overview

Private label ATMs, also known as white label ATMs are owned and operated by non-public companies. They are generally found in locations with high customer traffic, such as retail outlets, gas stations, and shopping malls. ATMs owned by financial institutions are regulated by Canada’s Office of Superintendent of Financial Institutions (OSFI) and the United States’ Federal Financial Institutions Examination Council (FFIEC). However, private label ATMs are not federally regulated. As such, there is an underlying perception that private label ATMs may be a target for money laundering.

In the United States and Canada, payment processors’ financial institutions are required by financial institution examiners and card network regulations to perform specific due diligence on each ATM operator and ATM source of funds provider (SOFP) for all installed terminals. ATM Operator Agreements and ATM SOFP Declaration Agreements must pass full due diligence for an ATM to be turned on for card acceptance.

---


Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

The purpose of ATM due diligence is two-fold: first, to confirm the identity of individual by utilizing a series of tools to cross-reference the information provided against available electronic records; and second, to confirm that the individual or business is an eligible ATM operator and ATM SOFP by evaluating risk-related attributes (such as liens, judgments, or bankruptcies) that identify derogatory information.

ATM due-diligence service of ATM operators and ATM SOFPs includes multiple inputs and data-point considerations to offer a comprehensive verification of an individual or business identity. A summary is provided below to demonstrate considerations that go into a final “pass/fail” score for each entity.

**Evaluation Criteria for Individuals**

**Individual Score** is used to verify an individual's identity. Attributes such as name, address, Social Security Number/Social Insurance Number, phone number, and date of birth are checked against each other, as well as a database to validate an individual.

**Fraud Score**:
- Three national consumer-credit reporting agencies
- Online utility, phone, and other consumer behavioral data sources
- Local, state/province, and federal government license, registration, and court-filing records

**Evaluation Criteria for Businesses**

**Business Score** is used to verify an organization’s existence. Attributes such as name, address, tax payer ID, and phone number are checked against each other as well as against a database to validate an organization’s existence.

**Business-Risk Score** is used to verify the business as well as incorporation.
- Data on corporate filings
- Better Business Bureau information
- Derogatory information (bankruptcy, liens, judgments, and so forth)

These processes are developed and implemented to identify and obtain sufficient due-diligence information to risk rate the ATM owner or operator, and implement a monitoring system.

This scenario illustrates how a private label ATM can be used to launder money:

A money launderer in the United States purchases a white label ATM and loads the ATM with cash proceeds from illegal businesses. The launderer, as an ATM operator, buys processing services from an ISO. The completed onboarding forms, ATM Operator Agreement and ATM SOFP Declaration Agreement, are submitted. ATM cash owner due-diligence check is completed, and ATM cash owner is registered with the payment networks. The ATM is enabled for processing. When a cardholder requests a withdrawal of funds through such an ATM, the withdrawal is authorized by the cardholder’s financial institution. The cardholder’s account is debited, the ATM dispenses currency in the withdrawal amount, and the money is transferred to the cash owners by the payment processor. This is considered a successful placement of dirty money in the financial system. The owner refills the currency in the ATM with currency withdrawn from its account or comingled with cash proceeds from illegal business.
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

Financial Institution and Processor Controls

- The cash owner’s financial institution’s transaction monitoring system flags the ATM deposits as an unusual activity on the account.
  - The cash owner’s profile is not set up for ATM deposit activity.
- Investigation and information sharing under Section 314(b) of the USA PATRIOT Act allows the processor’s acquiring bank and cash owner’s bank to work together.
  - The information on the cash owner’s Source of Funds Provider Declaration (SOFP) form is not consistent with the cash owner’s financial institution records.
    - The cash owner declared the initial ATM cash load came from its business bank account.
    - The review of the cash owner’s business bank account did not show the withdrawal of funds. No evidence is found to substantiate the cash owner’s signed SOFP declaration.

Actions Taken

- The acquiring financial institution and cash owner’s financial institution file suspicious activity reports (SARs) with FinCEN.
- The financial institution closes the cash owner’s account.
- The payment processor cancels the ATM cash owner’s service contract.

Merchant Due-Diligence Overview

Merchant underwriting is the first step in the merchant due diligence process. Without verification, bad actors can easily access the payment ecosystem and harm the industry’s reputation. Information collected during the underwriting process includes: the merchant’s history, verification of business structure, examination of processing statements, inventory reflects to sales reconciliation, operational data like average transaction amount, chargeback history, and beneficial owner information.

The traditional information coupled with the non-traditional data, such as the Better Business Bureau (BBB) report review or making a reverse phone search on Superpages.com, also helps to inform the merchant underwriting decision.

Money Laundering Goes Digital

In the past, laundering money required considerable effort by criminals. They needed to set up brick-and-mortar businesses, ensure they were running legitimately, keep clean books, and incur significant upfront operating expenses. However, money launderers are continually reinventing themselves and their methods. The adaptation to faster and frictionless payments has seen the shift to transaction laundering as the preferred method to place dirty money into the financial system.

Transaction laundering can be as simple as sharing merchant account information: The merchant acquirer registers an online pastry shop as a new low-risk merchant after it passes all KYC checks and screening requirements. However, the pastry shop serves as a front company (false, virtual storefront) for a website that sells counterfeit products. The most challenging transaction laundering scenarios are the ones with merchant collusion, using low-tech means for sharing the transaction data with no direct link between the two websites. The unregistered website owner passes transaction details to the registered merchant using a spreadsheet. The registered merchant (pass-through company)
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

manually inputs the information into the registered merchant account. Alternatively, it may be as sophisticated as embedding the same payment form used by the registered merchant website into one or more unregistered websites (funnel account).

These transaction laundering schemes are challenging the standard KYC checks and traditional monitoring. Online merchant service providers (MSP) have become increasingly aware of the deficiencies in the conventional anti-money laundering and fraud-mitigation methods. MSPs have responded to these new challenges by utilizing new resources and implementing emerging technology and processes to better monitor merchant risk. A digital solution requires a digital solution. Ongoing monitoring of online merchants and their transactional activity helps provide transparency to continuously validate important details like appropriate content, website security, and so forth. This level of transparency allows the MSP to know the merchant fully, be regulatory compliant, and keep on demonstrating compliance with card network rules.

The card networks are diligent in ensuring they are not used for illegal activities such as transaction laundering. They work closely with global law enforcement agencies, regulators, cardholders, and financial institutions, to identify industry trends relating to illegal activities. These card networks receive information that their network might be used to facilitate the purchase of an illegal product or service from various stakeholders, including law enforcement, cardholders, and customers. Whenever a card network becomes aware of a potential violation by a merchant, it conducts an internal investigation and notifies the acquirer of the possible card network rules violations. The acquirer is required to do its own investigation and respond to the card network inquiry. If it is confirmed that the merchant violated card network rules, the acquirer must ensure the merchant stops the illegal activity or be terminated from accepting card payment.

In order to proactively maintain compliance, acquirers and merchant service providers use the services of third-party digital-detection and prevention technology providers to monitor the risk of transaction laundering by taking these steps:

- Check the top-level domain list (TLD) of each merchant’s website for compliance. TLD is the very last section of an internet domain name after the dot, to help form a fully qualified domain name. For example, google.com is .com, but wikipedia.org is .org.
- Verify the actual goods and services advertised and sold on the registered merchant’s website,
- Validate the merchant category code on the approved merchant application versus the actual merchant category code of items or services offered.
- Be informed of every associated website of the registered merchant.
- Keep the archived evidence of the merchant’s violation, such as out-of-policy content with the timestamp.
- Find out if hidden websites are funnelling transactions to the registered merchant.
- Monitor for changes in the status of the merchant’s e-commerce activities continuously. Websites can be updated at any time and contain new associations, goods, services, payment options, contact information, and so forth.

The screening of these areas by a comprehensive automated AML digital-detection and prevention service can be beneficial to merchant service providers and their financial institutions in their fight against transaction and money laundering.
Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

Ultimate Beneficial Owner

People and organizations laundering money have learned through trial and error that anonymous shell companies can be used to pass scrutiny successfully. Their goal is to blend in and not appear to be risky. These shell companies usually are legal or incorporated entities and have little or no assets, few or no employees, and generally lack physical presence or operating locations.

From money laundering to cybercrime, anonymous shell companies are the leading element in most large-scale international fraud, money laundering, crime, and corruption. The fraudsters use concealment trickery as their primary tool.

However, payment processors are aware that newly formed shell companies do not have many of the red flags revealed during traditional due diligence or enhanced due-diligence process and, therefore, are granted approvals in many cases. That is, these shell companies and their deemed owners will not have negative news, registered legal matters, or a definite hit on the sanctions list database. In order to mitigate the risk, payment processors typically classify these entities as high risk.

AML legislations continue to evolve, and regulators, including FinCEN, have implemented zero-tolerance policies for financial institutions who work with payment processors. FinCEN\(^7\) requires MSP to verify the identity of legal entity customers, or the ultimate beneficial owner (UBO)—that is, the individual who controls the corporation, or either directly or indirectly owns 25% or more of the corporation’s shares. The UBO rule forces financial institutions to determine the identity of the beneficial owner(s) and perform AML/KYC checks on the individual to assess if the natural person poses AML/CTF risk to the financial institution and ultimately to the public. Beneficial ownership regulations cause many payment processors to review their processes. For example, due-diligence questionnaires may be enhanced to ask better questions; the listing of officers and directors with their contact information and the website address may be mandated.

TPPP Management Oversight Program

In the United States\(^8\) and Canada\(^9\), companies must comply with AML criminal codes, and it is unlawful to conduct or attempt to perform a financial transaction with proceeds known to be derived from illegal activity. Therefore, payment processors have AML responsibilities.

Payment processors are responsible for providing their customers’ bank accounts, and dollar amounts to the financial institution, and use the financial institution electronic transfer services to move the money to its customers’ bank accounts. If payment processors’ customers successfully use their services to inject dirty money into the financial

---


Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

ecosystem, and it is known, they may face penalties, fines, fraud loss, reputation loss, and even the loss of their business.

In light of these responsibilities, payment processors use the same processes and best practices as the financial institutions. They must make it part of their business processes to know the ultimate owners of all the relationships, whether it is a direct customer, the customer’s customer, or third-party vendor relationships within the payment ecosystem. It therefore becomes necessary to undertake additional due diligence and perform a deeper dive to confirm the verification of identity. A key example is the infamous Panama Papers, demonstrating the extent to which beneficial owners, that is, the actual persons who benefit from the dirty money, will go to conceal their identity by using anonymous shell companies.

Therefore, payment processors have an inherent self-interest to develop and perform the required due diligence on their customers, clients, or vendors to maintain their relationship with the financial institutions and, by extension, be compliant with the laws.

Also, most payment processors continue to automate their business processes to allow stronger compliance controls and the ability to capture more data consistently for all related categories of customers. If critical information is missing, such as the company’s beneficial ownership, system alerts will be generated enabling the analyst to apply their professional judgements based on their AML/CTF requirements and their expertise. These technology-enhanced procedures provide management with information and data about AML/CTF operating effectiveness and guide them in their decision making, oversight, overall staff management, and AML compliance regime.
### Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

#### Third-Party Payment Processor’s Risk-Based Assurance

<table>
<thead>
<tr>
<th>Phase</th>
<th>Objective</th>
<th>Example of Assurance Activity</th>
</tr>
</thead>
</table>
| 1. Planning and Risk Assessment | Obtain an understanding of the payment processor’s business, its reporting, policies, practices, and performance, and evaluate the company-level controls. | Review payment processor internal or external audits, and third-party due-diligence initiatives. Determine if they can be used. Obtain an understanding of the payment processor operations in order to develop the planned approach, including nature, timing, and extent of assurance procedures. Relevant documentation: 
- Organization chart
- Policies
- Procedures
- Risk assessment
- Training |
| 2. Testing             | Perform assurance procedures to obtain sufficient appropriate evidence on which to base the conclusion. | Perform walkthrough of the payment processor due-diligence process to gain an understanding of implemented controls and procedures. Focus areas:
- Customer identification
- Enhanced customer due diligence (EDD)
- Customer name screening
- Transaction monitoring systems and procedures
- Management information system
- Record keeping
- Decision making and governance
- Training
Testing of payment processor’s KYC, due diligence, and ongoing monitoring:
- Review the supporting documentation, policies, procedures, and practices based on acquiring financial institution and card network rules.
- Test representative sample of payment processor’s merchant, ATM cash owner, ATM operator, third-party service provider due-diligence files and transactions to confirm that documentation related to due-diligence measures is systematically requested, collected, and maintained on file in compliance with its policies, acquiring financial institution and card network rules.
- Test representative sample of payment processor staff training to confirm training is tracked, and knowledge is tested. |
| 3. Completion and Reporting | Form an assurance conclusion and provide other reporting as necessary. | Evaluate evidence. Prepare independent assurance report. |
Case Study
The case study illustrates that the payment processor uses the FFIEC BSA/AML Examination Manual as a guide¹⁰ and creates a management oversight program that improves the outcome of its independent audit, as well as provides useful information for their staff improvement and knowledge.

The Need
A third-party payment processor needs to meet new regulatory obligations with AML data, flexible screening, and monitoring.

The Objective
Implement a new payment option and be compliant with regulatory requirements.

TPPP Z's objective is to recognize and mitigate any financial-crime risk by implementing systems and controls that meet regulatory requirements.

TPPP Z was expanding into digital payment processing. TPPP Z was not equipped for the expansion of the increased customer base using its limited internal resources of people and tools. The deadline for ultimate beneficial ownership regulation was quickly approaching, which expanded the scope of screening required to include the requirement to know the beneficial owner. The existing manual monitoring process would not meet the demands of their fast growth. Also, the onboarding decisions were generating a large number of false positives, which had to be manually remediated.

Management stated it was necessary to review the existing AML/KYC framework, policies, and procedures. They wanted a system that would monitor risk profiles regularly and efficiently, following BSA/AML expectations. The system would automate ongoing monitoring and would proactively alert the compliance team when relevant risk changed, as well as reduce false positives by whitelisting entities once they were checked.

Following the review, TPPP Z implemented an effective customer management system to include an update to policies and procedures, customer identification, customer enrollment, customer due diligence, persistent monitoring, reputation monitoring, deposit return, chargebacks level monitoring, and reporting.

The customer identification program required the group to utilize many functions across the company to assist in accurately identifying the customer. Customer identification oversight includes the relationship management team, AML operation team, and compliance.

TPPP Z received a merchant application from a newly formed shell company. The initial due diligence identified the applicant as part of a larger group of companies, consisting of those registered in various jurisdictions with a lack of AML oversight. The prospective merchant was not responsive to TPPP Z's employees' e-mails and telephone calls requesting additional information regarding the people acting as representatives of the shell company. Furthermore, TPPP Z could not verify the beneficial owner and who controls the shell company. The merchant application was not approved for merchant services.

Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

Financial institutions and their payment processing customers who demonstrate that appropriate compliance programs are in place may reduce the severity of supervisory enforcement action if it is subject to financial crimes such as breach of anti-money laundering regulations.

Conclusion

In conclusion, while payment processors do not fall within the United States’ Bank Secrecy Act and Canada’s Proceeds of Crime (Money Laundering) and Terrorist Financing Act, payment processors must comply with AML criminal codes in the United States\(^\text{11}\) and Canada,\(^\text{12}\) to do business with and maintain ongoing relationships with regulated financial institutions. They are required to develop effective risk-management AML/CTF policies and procedures, and undertake some of the very stringent risk-assessment and due-diligence procedures for their customers and third-party vendors. Also imperative to their ongoing effectiveness, they will need to enhance their ongoing monitoring systems to keep abreast of changing AML/CTF regulatory requirements imposed on the financial institutions, the regulators, and card networks. Payment processors and their alliances recognize that it is their collective responsibility to do their very best to prevent and detect money laundering and disrupt terrorist financing by being diligent during customer onboarding, and by implementing current technologies and methods to perform ongoing monitoring. External oversight and supervision by the financial institutions and card networks assure users of the card-payment ecosystem that third-party payment processors adhere to an adequate set of industry, risk-management, and anti-money laundering standards.

---


Anti-Money Laundering and Third-Party Payment Processors (TPPPs)

References


