Anti-Money Laundering Training Program

H&R Block Canada, Inc.

H&R BLOCK

DCBank

Objectives

- Define money laundering and terrorist financing.
- Identify Canadian government organizations involved in anti-money laundering (AML) and counter-terrorist financing (CTF).
- Identify the client requirements and records required to open a DC Bank account.
- Recognize and understand the importance of “Know Your Client” (KYC) rules.
- Recognize and identify suspicious transactions (attempted and completed).
- Understand the various penalties for non-compliance.

About the Proceeds of Crime (Money Laundering) and Terrorist Financing Act

The objective of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) is to help detect and deter money laundering and the financing of terrorist activities.

Your Responsibilities as an H&R Block Canada Inc. (H&R Block) associate:

- You must understand and implement requirements for:
  - Record-keeping
  - Client identification
  - Reporting of suspicious transactions
- You must comply with the PCMLTFA and its supporting regulations

Non-compliance with the PCMLTFA can result in criminal charges or administrative fines.

DC Bank's Compliance Program establishes a mandate that H&R Block associates are able to demonstrate an understanding of money laundering and terrorist financing through the practice of their organization's policies and procedures.

Compliance Regime

DC Bank supports the fight against money laundering and terrorist financing and has adopted a compliance regime to prevent its financial services from being used in promoting criminal activity.

DC Bank complies with all laws and regulations relating to money laundering and terrorist financing.

Audits and reviews are conducted to ensure anti-money laundering (AML) and counter-terrorist financing processes and documents are compliant and meet regulatory requirements.

The DC Bank compliance regime includes:

- A compliance officer (DC Bank Compliance Department).
- Written and up-to-date AML/CTF policies and procedures.
- Risk assessment, as well as the documentation and implementation of mitigation measures to address risks.
- AML compliance training.
- Regular review all AML/CTF compliance policies and procedures.

Government Organizations

There are two main Canadian Government organizations involved in detecting and deterring money laundering and terrorist financing in Canada:

FINTRAC – The Financial Transactions and Reports Analysis Centre of Canada

- Canada's financial intelligence unit (FIU) was created in 2000 as an independent agency reporting to the Minister of Finance. Its mission is to contribute to the public safety of Canadians and help protect the integrity of Canada's financial system through the detection and deterrence of money laundering and terrorist financing.
- FINTRAC ensures compliance of reporting entities with the legislation and regulations including record keeping and client identification requirements.

OSFI – Office of the Superintendent of Financial Institutions

- Created to contribute to public confidence in the Canadian financial system.
- OSFI performs regulatory audits on financial institutions.
- OSFI also requires that federally regulated financial institutions are compliant with their guidelines.

Accountabilities

Criminal Penalties include:

- Failure to report suspicious transactions or submit a terrorist property report: up to $2 million and/or 5 years imprisonment.
- Failure to meet record keeping requirements: up to $500,000 and/or 5 years imprisonment.
- Failure to provide assistance or provide information during a FINTRAC compliance examination: up to $500,000 and/or 5 years imprisonment.
- Disclosing the fact that a suspicious transaction report was made (tipping off), or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to 2 years imprisonment.

Civil Penalties: Each violation is classified as a minor, serious or very serious violation. The history of compliance by the associate with the *PCMLTFA* will be taken into account in determining the amount of a penalty.
Subject to the PCMLTFA, the range of penalties in respect of a violation is:

(a) $1 to $1,000 in the case of a 'minor' violation;
(b) $1 to $100,000 in the case of a 'serious' violation; and
(c) $1 to $500,000 in the case of a 'very serious' violation.

What is Money Laundering?

Money laundering is the process of transforming the proceeds of crime (dirty money) into “clean” money or other assets. This is done by moving the money through legitimate businesses. Once complete, the money cannot be easily traced to its origin.

Criminals may launder money to evade taxes that would be imposed on earnings, avoid seizure of their wealth and avoid prosecution

The main categories of money launderers include:

- Organized Crime Groups
- White Collar Professionals

Three Stages of Money Laundering

PLACEMENT: The entry of illegal funds into the financial system to relieve the criminal of holding and guarding dirty money. Placement techniques include structuring deposits in amounts to evade reporting requirements or co-mingling currency deposits of legal and illegal enterprises.

LAYERING: Hiding the origin of the funds through multiple and or complicated transactions. It is used to try and disguise any link with the original crime that generated the dirty money.

INTEGRATION: Exit of laundered funds from the financial system without attracting suspicion. The loading of illegal funds onto a prepaid card is an example of integration.

Three Stages of Money Laundering - Examples

PLACEMENT

H&R Block Canada has very little direct involvement with placement. A possible scenario is the customer requesting H&R Block make a Canada Revenue Agency payment, on their behalf, for tax owing via cash payment.

LAYERING

Illegal income can be hidden at tax preparation time by declaring dirty money as clean income. This can be evident from suspicious types of income statements, fraudulent T-4 slips or phony pay stubs. Other indicators can also include:

- Large declared income for an individual who cannot explain source of funds.
- Greater than normal number of income statements provided for the stated occupation.
- Sizeable income reported from tax haven countries.

INTEGRATION

Tax refunds could be viewed as receiving legitimate funds from the process of laundering dirty income or taking advantage of illegal deductions. Suspicion of tax fraud should be reported, this is why it is important to pay close attention to the documentation used to prepare the customer's tax return.

What is Terrorist Financing?

Terrorist financing (proceeds ***for*** crime) is the process by which funds are provided for terrorist activity.

Large amount of funding for terrorism activities comes from legitimate sources, this is why terrorist financing is sometimes depicted as the reverse of money laundering.

Terrorist financing involves moving legitimate funds into terrorist hands.

Terrorist groups are monitored by OSFI (Canada) and the United Nations. Terrorist names are posted publically on their respective websites. DC Bank regularly consults these lists.

Reporting suspicious behavior is very important, regardless of if it is for money laundering or terrorist financing

Know Your Client

In taking proactive measures to prevent money laundering or terrorist financing, it is important to ensure information obtained from required identification documents, reports and records is as accurate and effective as possible.

The Know Your Client (KYC) Policy refers to the documentation which sets out DC Bank's approach to ensure effective identification, verification and monitoring of clients.

The Principal Objectives of a KYC Policy include:

1. Ensuring that only legitimate clients are provided with DC Bank products.
2. Verifying the identity of clients through approved, reliable, and independent documentation.
3. Ensuring that the risks posed by each client are understood.
4. Managing the risks posed by identifying the source of funds, occupation, intended use of account, or suspicious behavior and transactions.

Know Your Client (KYC) Policy Elements

Acceptance	The point at which a new client is accepted or rejected is the easiest point at which the risk of dealing with illegal money can be avoided.
Identification	Establishing the identity of clients is the easiest way to help protect H&R Block and DC Bank from unknowingly doing business with a terrorist or criminal.
Verification	Verify that clients are who they say they are by verifying original government issued Identification or an original identification document from a primary or secondary form of ID in the Acceptable ID Policy.
Behaviour	Identify and report any suspicious behavior or unusual activities.
Risk	Know where the money came from (source of funds).

Identifying Your Client – Proper ID

Identification of an individual is required at the time the account is being opened.

1. Identifying your Client:

Verify the clients identity by collecting two pieces of personal identification. At least one must be from the Primary Identification List. It is preferred that the second piece be government issued identification also.

ID must:

- Be in the same name and image as the applicant.
- Not be expired.
- Have a unique identifier.
- Be an original; NO photo copies.
- Not be substantially damaged or appear to be altered.

If the client cannot provide ID, an account cannot be opened

Identifying Your Client – Third Party Accounts

2. Ensure client is NOT a third party

Always ask the client if they are opening an account for themselves or on behalf of someone else (Third Party).

What is a Third Party?

- A Third Party is an individual or entity, other than the account holder who directs what happens with the account.
- If only one individual is present but that person is acting on someone else's instructions, there is a third party involved.

Note: A person conducting a transaction on behalf of an elderly or disabled person is considered to be a third party.

DC Bank does not accept Third Party accounts; If you determine this is a Third Party account DO NOT OPEN THE ACCOUNT.

Identifying Your Client – PEFPs and PEPs

3. Ensure client is not a Politically Exposed Foreign Person (PEFP) or a Politically Exposed Person (domestic) PEP.

A PEFP or PEP is defined as a person who holds or has held one of the following offices or positions in or on behalf of a foreign country or domestically:

- Head of state of government
- Member of the executive council of government or member of a legislature
- Deputy minister or equivalent risk
- Ambassador or an ambassador's attaché or counsellor
- A military general (or higher rank)
- President of a state-owned company or a state-owned bank
- Head of a government agency
- A Judge
- Leader of president of a political party represented in a legislature
- A prescribed family member of a person listed above

Due to their political position, these individuals may be susceptible to corruption and/or bribery.

Identifying Your Client – PEFPs and PEPs con't

You must take reasonable measures to determine if the client is a PEFP or PEP and check the correct box on the Deposit Account Agreement. You must read the PEFP or PEP description to the customer or give the customer the Deposit Account Agreement to read the description and then ask the customer directly, "Does this description apply to you?"

If the client says "Yes" they are a PEFP/PEP, record the information but **DO NOT OPEN THE ACCOUNT**

DC Bank does not accept PEFPs or Domestic PEPs

Identifying Your Client – Occupation

Occupational Information:

You are required to ask where an applicant works and his/her occupation or principal business and then choose the corresponding occupation from the drop-down menu.

If the drop down menu option does not specifically describe the occupation, choose one that best applies and then manually write additional information on the DC Bank Agreement form.

It is a requirement that occupation information be as descriptive and specific as possible. For example, “contractor”, “owner”, “self-employed” are not specific enough as they do not indicate the type of business the client is in. If the customer is retired, the customer’s previous occupation such as “retired teacher”, “retired book keeper on CPP”; “unemployed on social assistance”, or “unemployed on disability pension”, etc., should be written on the form.

The field “occupation” is very important because it assists in determining source of income.

Completing an Application

If a client refuses to provide all information required, a bank account CANNOT be opened. An associate CANNOT issue a prepaid card, load a card or process any transaction without the client providing all information required.

Place a copy of the signed **Agreement/Terms and Conditions** in a separate file and store in a secure environment. All records must be kept in this file. Files must be kept for a minimum of seven years.

Please ensure that the customer receives a copy of the **Agreement/Terms and Conditions**.

If proper identification information is not collected and recorded, large fines can be levied against H&R Block, you personally as an H&R Block associate, and/or DC Bank.

Suspicious Activity

There are two types of suspicious transactions:

A **completed suspicious transaction**: a transaction that has occurred and is finalized

A **suspicious attempted transaction**: an incomplete transaction where after the process was started the DC Bank employee or H&R Block associate decides to cancel for a specific reason.

Both suspicious transactions and suspicious attempted transactions must be reported and escalated to your compliance department. Failure to report a suspicious transaction when you have reasonable grounds may result in criminal penalties or fines to H&R Block, you personally as an H&R Block associate and/or DC Bank

http://www.fintrac.gc.ca/publications/guide/guide2/2-eng.asp#s7

Examples of Suspicious Activity

FINTRAC has provided a list of suspicious transaction common indicators. These indicators include:

- Client admits or makes statements about involvement in criminal activities.
- Client is accompanied and watched.
- Client uses aliases and a variety of similar but different addresses.
- Client indicates he/she has been to two or more locations on the same day.
- Client states he/she does not have a local address but you suspect they reside locally.
- Client tries to use a post office box or General Delivery address or other type of mail drop address instead of a street address *when this is not the norm for that area*.
- A client starts the process for a Pay With Refund but then leaves the branch when asked for identification.
- Client provides false information or information that you believe is unreliable.
- Stated occupation of the client or the client's financial standing is not in keeping with the level or type of activity (for example a student or an unemployed individual who undertakes a large-value transaction).

Suspicious Transactions: Things to Remember

When reporting a suspicious transaction (completed or attempted) or considering making a report to the Compliance Department remember the following:

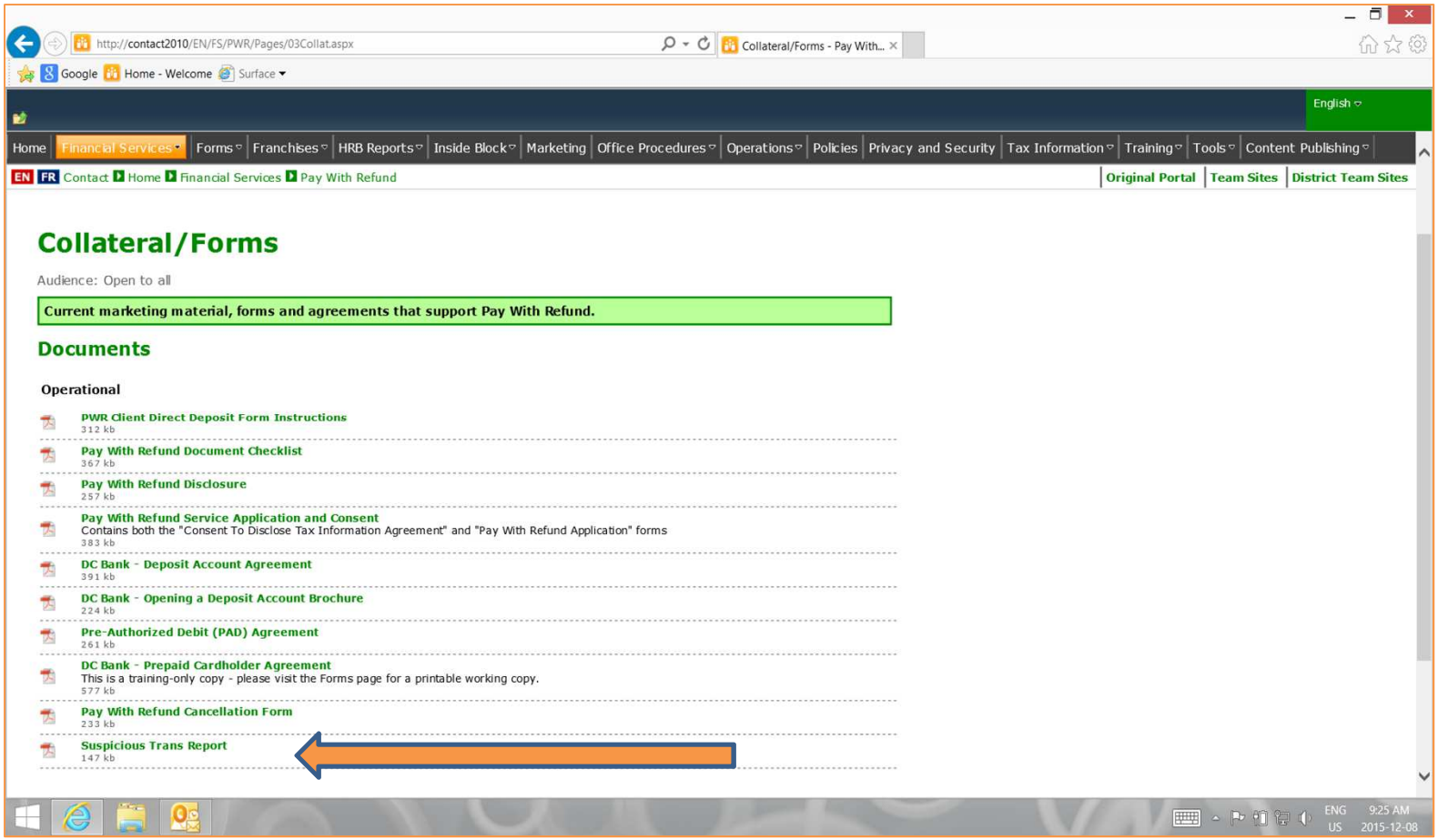
The more information you know about your customer, the better position you will be in to determine whether the transaction is suspicious.

To report a suspected suspicious or attempted suspicious transaction, the **Suspicious Transaction Form** must be immediately emailed to the H&R Block Compliance Department at:

complianceAML@hrblock.ca

Where is the Form Located?

Path: CONTACT/Financial Services/Pay with Refund/Collateral Forms/Operational



Tax Evasion

Tax evasion is the term for the illegal nonpayment or underpayment of tax.

On July 12, 2010 tax evasion became a money laundering offence; because of this change you must now report any suspicious activity that indicates your client may be involved in tax evasion.

Indicators of tax evasion include:

- Transfer of large sums of money to foreign/low tax jurisdictions.
- Transactions involving a country known for highly secretive banking and corporate law.
- Client and other parties to the transaction have no apparent ties to Canada.
- Client makes reference to transactions as ones being taken to try and avoid taxes.

Tax avoidance is the legal usage of the tax regime in a single territory to one's own advantage to reduce the amount of tax that is payable by means that are within the law. As tax avoidance is legal, it does not need to be reported as suspicious.

Reminder: Tipping Off

FINTRAC Guideline 2, Suspicious Transactions: states, You are not allowed to inform anyone, including the client, about the contents of a suspicious transaction report or even that you have made such a report, if your intent is to harm or impair a criminal investigation. This applies whether or not such an investigation has begun.

Because it is important not to tip your client off that you are making a suspicious transaction report, you should not be requesting information from the individual conducting or attempting the transaction that you would not normally request during a transaction.

FINTRAC imposes monetary penalties on those who tip off anyone about a suspicious transaction report if the intent is to harm or impair a criminal investigation.

NOTE: By reporting to FINTRAC, no criminal or civil proceedings may be brought against you for **making a report in good faith**.

Exercise – Suspicious Transactions

Scenario:
A new client meets with you to have a tax return prepared. This client is not a regular and you do not recognize him. You note the following things:

- The client is abrupt and irritable and is overly impatient to have the process completed, collect the 'possible' refund, and leave.
- During the review of the customer's tax documents, it is noted the individual has generated a lot of revenue during the year and some of this revenue was generated internationally.
- When asked what the customer does for a living, the customer states they are a self-employed consultant, providing no further information while citing privacy regulations.
- When asked for clarification on certain documents, the explanations do not always make sense.
- Hand written invoices and questionable supply and deduction receipts are submitted.
- The customer appears overly thrilled with receiving a small return and is anxious to leave.

Can you spot the suspicious indicators?

Exercise – Suspicious Transactions, Indicators

In this situation, the indicators of suspicious activity include:

- The customer's demeanor suggests their guard is up and that they might be hiding something.
- Some income statements provided were from international sources.
- Customer provided limited information regarding their employment.
- Customer puts up privacy regulatory walls to keep you in the dark
- Some of the documentation appears questionable.
- The customer is vague in explaining the relevance of certain documents.
- The customer's final response after receiving a return does not fit with the situation and the customer's behavior through the tax preparation process.

Remember: Any one indicator may not be suspicious, but you should consider all indicators and the entire situation when considering if there are reasonable grounds to suspect the client may be involved in a suspicious transaction like tax evasion. If you do conclude that the transaction is suspicious, you should contact the H&R Block Compliance Department as soon as possible at:

complianceAML@hrblock.ca

Questions?

Please contact the compliance department at:

ComplianceAML@hrblock.ca