Combating the Layering and Integration of Money Laundering by Debit Card

Sun, Qian

CAMS-Audit Advanced Certification White Paper
# Table of Content

1. BACKGROUND INTRODUCTION

2. DEFINITION AND FEATURE OF DEBIT CARD
   2.1 Card Classification
   2.2 Stakeholders and Roles
   2.3 Features of Debit Card

3. TRANSACTION TYPE AND SCENARIO
   3.1 Transaction Types
   3.2 Transaction Scenarios

4. TYPICAL MONEY LAUNDERING TECHNIQUE
   4.1 Placement
   4.2 Layering
   4.3 Integration

5. DIFFICULTY IN DEBIT CARD AML
   5.1 Overseas Debit Card
   5.2 Cooperation and Information Sharing
   5.3 Accountability Awareness
   5.4 Bucket Effect

6. APPROACH TO MITIGATE MONEY LAUNDERING RISK
   6.1 Establishing Universal standards and Upgrading
   6.2 Cooperation in Investigation and Information Sharing
   6.3 Implementation, Regulation and Law Enforcement

7. TESTING PROCEDURE
   7.1 Set Expectation and Recognize Environment
   7.2 Evaluate Technical Compliance
   7.3 Assess Implementation Effectiveness
   7.4 Define Residual Risk and Propose Improvement Suggestion

8. CONCLUSION

9. REFERENCE
1 BACKGROUND INTRODUCTION

Debit cards are a basic and popular financial instrument all over the world, and they have inevitably been used throughout all three stages of money laundering. In recent years, along with new technologies adopted in the financial system, debit card payments have become a very convenient and efficient option, particularly in Asia-Pacific countries and regions where debit cards are widely used in not only cash withdrawal but also purchase transactions.

In addition to many researches that have been introduced to address and mitigate money laundering risks related to debit cards, this article will focus on the layering and integration stages. This article will first analyze the vulnerability of debit cards in money laundering, explain how debit cards could be used to facilitate money laundering (particularly in the layering and integration stages), and encourage a holistic solution through the joint efforts of all stakeholders. In addition, this article will propose a solution for testing and auditing procedures.

The expected audience of this article should be debit card stakeholders, including card issuers, card acquirers, cardholders, merchants, regulators, and other financial or non-financial institutions whose services are based on debit cards.

2 DEFINITION AND FEATURE OF DEBIT CARD

2.1 Card Classification

"A bank card is typically a plastic card issued by a bank to its clients that performs one or more of a number of services that relate to giving the client access to funds, either from the client's own bank account, or through a credit account."

In fact, there are multiple dimensions to classify a bank card; for example, it can be classified as a:

- Debit or credit card based on the difference in source of funding
- Plastic or digital cards based on whether it has a physical presence
- Chip or magnetic cards based on whether the carrier of data and information is a microchip or a magnetic strip, and so on.

Debit cards are typically issued by a bank when the cardholder registers for a savings or checking account. Unlike credit cards, the funds disbursed from a debit card are from the account balance that the cardholder deposited previously rather than a line of credit offered by the bank.

2.2 Stakeholders and Roles

---

1 https://en.wikipedia.org/wiki/Bank_card
From an AML perspective, there are generally five roles involved in the debit card world: issuer, acquirer, cardholder, merchant, card scheme or switching center and regulator.

- An issuer can be a bank, a non-bank financial institution, or even a non-financial entity. For example, a gym or a barbershop may issue a card to a client. As for a debit card, the issuer will have to be a bank because it has to be issued based on a savings account and in most cases only banks can absorb savings from a crowd.

- An acquirer is an entity that accepts the usage of the debit card. For example, when a debit card is used to withdraw cash from an ATM, the owner of the ATM is the acquirer.

- A cardholder, as its literal meaning, is the holder of a debit card and would normally should be the owner of the savings account tied to the debit card.

- A merchant is a relative concept to a cardholder. For example, when a debit card is used for a POS transaction to purchase goods or services, the seller or provider is the merchant.

- A card scheme or switching center is based on a standard interchange technical standard and it facilitates the usage of debit cards among different issuers, merchants and acquirer located in different countries.

- A regulator is the same as its role in any industry, which supervises and regulates debit card activities.

2.3 Features of Debit Card

**Portability.** If we only consider physical cards, a debit card is a papery piece of plastic (sometimes metal) no larger than 6cm x 10cm, which makes debit cards very portable. Cardholders can keep a dozen debit cards within a small purse in hand without been inquired by any customs inspector. There are cases of smuggling cash, goods, drugs, etc., but not debit cards.

**High Value.** Because debit cards are linked to saving accounts, the available value of a debit card is equal to the outstanding balance of the savings account, and such balance is reloadable.

**Wide scope of acceptability.** The acceptance network of debit cards is now covered almost everywhere. For example, according to the descriptions provided on official websites of top three international card schemes, VISA says it "connect[s] consumers, businesses, banks and governments in more than 200 countries and territories worldwide."² UnionPay says it "has enabled card acceptance in 160 countries and regions,"³ and MasterCard says it connects "

²[https://usa.visa.com/about-visa.html](https://usa.visa.com/about-visa.html)
consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories.\textsuperscript{4}

**Support of various use pattern.** Debit cards can be used to deposit or withdraw cash, to fund a payment transaction, to send or receive, to transfer, etc. They are accepted by terminals like POS and ATMs, and by intangible interfaces like internet website and mobile phone applications.

Debit cards have become the primary vehicle for conducting transactions in countries where “paper” checks have not been a form of payment traditionally. According to a report published in China, in 2015 there was a total of 5.61 billion bank cards issued—5.09 billion of these were debit cards, which means approximately each Chinese citizen owns four debit cards. The report also indicated that 85.23 billion bank card transactions occurred in 2015 and the total amount is about $207 trillion, among which 15.46 billion transactions with a total amount of about $200 trillion were conducted by debit cards.\textsuperscript{5}

### 3 TRANSACTION TYPE AND SCENARIO

#### 3.1 Transaction Types

\textsuperscript{4}https://www.mastercard.us/en-us/about-mastercard/what-we-do.html

\textsuperscript{5}http://www.zgyhy.com.cn/zixun/2016-09-22/2966.html; The Bank Card Industry Development Blue Paper (2016), Bank Card Committee of Bank Associate of China
Deposit, withdrawal, transfer, purchase—these words all have more than one definition, but within this paper we specify each.

“Deposit” refers to a transaction that will add money into a checking account via a debit card. On the other hand, withdrawals refer to a transaction that will deduct the money in saving accounts and turn such amount into cash. Transfers are two-way transactions (sending and receiving). A purchase is a transaction transfers money from a buyer's saving account to the counterparty seller's account. The difference between transfers and purchases is that the latter is based on a genuine trading background (goods or services are actually sold and bought) while the former is not.

### 3.2 Transaction Scenarios

There are multiple dimensions of explanation related to transaction scenarios, in fact a lot of financial institutions, particularly technology companies' businesses, are built up on the development of transaction scenarios. Within this article, I classify transaction scenarios into two categories: card present and card not present.

Card present refers to transaction scenarios where a physical debit card is presented to whoever or whatever accepts the card. For example, if a cardholder walks into a bank to make a deposit at the bank counter, he/she must provide the card to the teller. In addition, when a cardholder is purchasing goods at a physical store like a supermarket or a mall, he/she will have to provide the card to the cashier and when a cardholder wants to withdraw cash at an ATM, he/she needs to insert the card into the machine.

On the other hand, card not present refers to transaction scenarios where the presence of card is not needed. For example, if a cardholder wants to purchase goods from an online store via the internet, he/she does not need to provide the physical card to anyone but input several pieces of information on his/her computer or mobile phone via certain interfaces. The cardholder can also make a purchase by calling a merchant’s sales hotline and complete the payment by answering IVR (interactive voice response) questions related to the card information. Furthermore, if the cardholder has confirmed a recurring payment agreement, his/her issuer will automatically complete the payment transaction on behalf of the cardholder.

### 4 TYPICAL MONEY LAUNDERING TECHNIQUE

#### 4.1 Placement

In this stage, money launderers mainly have two objectives: to obtain a debit card without exposing identity and to add illicit money into a debit card. Unfortunately, the underground market of debit cards and identity is now an established business practice by which money launderers can easily and effectively achieve their first objective. Money launderers can always hire
people to act as their agent. Each of these agents (smurfs) normally will be
directed to deposit cash into multiple debit cards at different ATMs. Now money
launderers have successfully put their dirty funds into a globally connected
financial network.

4.2 Layering

Most frequently, the first step of layering is funds transfer among a mass of debit
cards, which can be done either online or an ATM. Many debit cards now have
enabled online transfer functions. If you know the card number and the
password it could be enough to initiate an online transfer. Sometimes a third
verification tool, such as a digital certificate or a token may be required, and
sometimes the IP address used may be traced, but these verifications methods
only created very few challenges to money launderers.

After sophisticated transfers, the origin and movement track of funds have
become a tremendously difficult job for anyone who wants to trace it.
Sometimes the money launderers may have a designed road map for such
transfers in advance, like a logistics plan. But in most cases, typically when the
layering network is too big, money launderers themselves will only set the
starting and ending point while the progress between are almost random, which
increases the difficulties in tracing, predicting and intercepting.

Now, money launderers can use debit cards to withdraw cash at ATMs to finish
the layering. They also can make the layering even more complicated by
conducting purchasing transactions via POS at a merchant, and ask for a
refund or re-sell the purchased goods somewhere else. The merchants can be
normal, but in some cases, such merchants are controlled or conspired with the
money launderer.

Due to the aforementioned features of debit cards, money launderers can bring
multiple debit cards when traveling cross-borders without being inspected. This
means that all of the ATM withdrawals or POS purchases can be easily
conducted overseas based on the network of card scheme from the country
where the dirty money is originated.

4.3 Integration

There is not a clear boundary between layering and integration when using
debit cards for money laudnering. For example, when a debit card is used to
withdraw cash from an ATM, if the cash is used as normal money, the
withdrawal can be considered as the process of integration; however, if the cash
is deposited and transferred again, it can be considered layering. The same
logic applies for purchases. Another scenario is that debit card funds can be
used to pay back a loan, or used as a pledge to apply for loan.
5 DIFFICULTY IN DEBIT CARD AML

In combating money laundering by debit cards, the industry now faces four major difficulties.

5.1 Overseas Debit Card

The first concern is about the cross-border transportation of funds in debit cards. As previously explained, when crossing borders you will not be inspected for carrying multiple debit cards. At present, there are many countries that have a quota for cash per person when travelers want to enter and/or exit. For example, China permits travels to carry 20,000 CNY or $5,000 equivalent without additional report\(^6\) (the U.S requires explanation and will need to file a report if someone carries cash exceeding $10,000\(^7\), etc. However, if the funds are deposited in a debit card already, travelers can carry the cards along with them because a customs inspection officer has no idea about the balance of such cards.

Other bad news is that since quite a lot of debit cards are magnetic cards, money launderers can transcribe the magnetic strip data into a digital storage tool like a hard disk or flash drive. After these storage tools were brought to the destination country, money launders can transcribe the data back to any magnetic cards they obtained from local card issuers, and use these cards to withdraw cash at ATMs.

5.2 Cooperation and Information Sharing

The second concern is information sharing in verification and investigation of debit card transactions.

Know your customer (KYC) is the foundation of AML and financial institutions and designated non-financial business and personnel (DNFBPs) all know the importance of it and have accumulated quite a lot of experience in recognizing red flags when conducting KYC and due diligence. However, despite that the concept of know your customer’s customer has become more and more popular, many institutions still have not brought it into practice or have ignored it. This is insufficient to build a customer profile from the view of risk-based approach. For example, if an issuer bank only pays attention to the individual cardholder of a debit card issued by the bank, but has no idea about who are the merchants that the cardholder frequently visits, there is no way that the issuer could have a thorough understanding of its customer. And if the cardholder in this example is an entity, the issuer needs to know the major business counterparties of this entity so to establish a profile of this customer. Or else the issuer will not be able to recognize the red flags when monitoring.

\(^6\)http://www.customs.gov.cn/publish/portal123/tab60957/info761684.htm, Custom of the People’s Republic of China

\(^7\)https://www.cbp.gov/newsroom/local-media-release/cbp-reminds-public-currency-reporting-requirements, U.S Customs and Border Protection
Besides willful blindness, know your customer’s customer also has practical difficulties. Since banks can act as both issuer and acquirer, it is much easier to verify the identity of a cardholder when a debit card is used at an ATM or POS that is owned by the same bank. It is not too hard to verify within the same jurisdiction even if the issuer and the acquirer are from different banks because they all follow the same law and regulation. But if the scenario comes to a cross-border transaction the differences (AML laws and regulations) between the two jurisdictions, may cause a problem. For example, if a debit card issued in Thailand is used in the U.S., the acquirer in the U.S will have no idea about who the cardholder is and whether or not the transaction is consistent with historical behavior, and vice versa.

5.3 Accountability Awareness

The third concern is about the awareness of using debit cards in money laundering. It has two levels of concern: one is that some issuers will pay more attention to the authentication rather than the verification of the purpose of a debit card transaction. Some issuers may even intentionally turn a blind eye when monitoring debit card transactions as long as the transactions do not look fraudulent. The other meaning is, as aforementioned, identity and debit card selling in the underground market reflects the fact that many civilians and authentic cardholders do not care about the consequences caused.

5.4 Bucket Effect

The last concern is that because debit card are a fundamental financial instrument, many financial services use it and if the issuing and monitoring of the debit card is not appropriate and sufficient, all financial services will fail their AML obligation. For example, online express pay is a product mainly provided by non-bank institutions and customers can enroll their debit card with an account registered with these providers, and after the enrollment, customers can conduct a payment by providing the account number and PIN. This means that although the transactions look like they are based on the debit card, the authentic cardholder may have no idea about the transactions. Like the enrollment of online express pay, many other financial services also rely on the debit card to verify the identity of their customer, sounds like a single sign on. Such practices make the debit card industry larger and more complex, and also more vulnerable to money laundering especially when some of the participants do not have a sound AML capability.

6 APPROACH TO MITIGATE MONEY LAUNDERING RISK

In order to cope with the difficulties and concerns aforementioned, a holistic AML framework based on the cooperation of all participants in the debit card industry is needed. The efforts can be achieved from the following perspectives.

6.1 Establishing Universal Standards and Upgrading
The objective of setting universal standards is to avoid any barricade that may hinder AML practices in different jurisdictions, which is not contradictory to the risk-based approach. There are already several internationally recognized AML standards including FATF Recommendations and Interpretive Notes, guidelines and consultative documents published by the Basel Committee on Banking Supervision, etc. If all participants in the debit card industry can adopt such standards into their AML framework, communication and cooperation will be smoother.

The first standard could be KYC because it is the foundation of AML. In terms of this issue, Basel has published documents indicating how banks should collect information for identification purposes respectively for natural persons and legal persons:

For natural persons

<table>
<thead>
<tr>
<th>At a minimum</th>
<th>Potential additional information (on the basis of risks)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal name (first names and last name);</td>
<td>Any other names used (such as marital name, former legal name or alias);</td>
</tr>
<tr>
<td>Complete permanent address, whenever applicable;</td>
<td>Professional address, post office box number, e-mail address and landline or mobile telephone numbers;</td>
</tr>
<tr>
<td>Nationality, an official personal identification number or other unique identifier ;</td>
<td>Resident status;</td>
</tr>
<tr>
<td>Date and place of birth.</td>
<td>Gender.</td>
</tr>
</tbody>
</table>

For legal persons

<table>
<thead>
<tr>
<th>At a minimum</th>
<th>Potential additional information (on the basis of risks)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name, legal form, status and proof of incorporation of the legal person;</td>
<td></td>
</tr>
<tr>
<td>Permanent address of principal place of the legal person’s activities;</td>
<td></td>
</tr>
<tr>
<td>Official identification number (company registration number, tax identification number);</td>
<td>Legal entity identifier (LEI) if available;</td>
</tr>
<tr>
<td>Mailing and registered address of legal person;</td>
<td>Contact telephone and fax numbers.</td>
</tr>
<tr>
<td>Identity of natural persons who have authority to operate the account and who</td>
<td>Identity of relevant persons holding senior management</td>
</tr>
</tbody>
</table>

---

8Basel Committee on Banking Supervision; Consultative Document; General guide to account opening; July 2015; page 6
exercise control of the legal person through ownership or other means. In the absence of a natural person, the identity of the relevant person who is the senior managing official.

| Identity of the beneficial owners (according to relevant FATF standards and paragraph 13 of this annex); |
| Powers that regulate and bind the legal person. |

FATF has explained the reliance on third parties: "Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party."⁹ This standard will help a lot to solve the effect as aforementioned.

The second standard could be legislation about prohibiting the selling or renting of personal identity information, as well as financial instruments like debit card. If such activities are globally recognized as illegal, while judicial cooperation is in effect, underground market for identity and debit card could be limited.

The third standard could be the technology standards. For example, the mandatory migration of magnetic card to chip card so that money launderers are unable to transcribe and reproduce debit card overseas. Another example is the application of biological characteristics. Issuers can collect the bio characteristics of the cardholder, while acquirers can install a bio characteristics verification tool on the acceptance terminals.

The forth standard could be the limitation of financial instruments when used overseas. For example, according to Chinese regulation, each debit card issued in the mainland of China has a daily quota of 10,000 CNY and annual quota of 100,000 CNY for overseas cash withdrawal.¹⁰ This kind of limitation increased the costs of money launderers.

### 6.2 Cooperation in Investigation and Information Sharing

Transaction monitoring and reporting is an essential component of AML. It is a commonly encountered difficulty when investigating suspicious activity or transactions that involve cross-border objects. At present, many countries and/or their FIUs have established mutual legal assistance framework based

---

⁹The FATF Recommendations; February 2012, Recommendation 17; page 20
on the memorandum of understanding, which is great. However, this kind of mechanism often applies to critical money laundering cases and is low-effective for routine investigations.

To solve this problem, international card schemes can play an important role. For example, if card schemes are required to submit SARs to applicable FIUs, they will coordinate both ends of issuer and acquirer in the investigation of cross-border transactions based on the card scheme's rule as long as applicable laws do not prohibit it.

Besides specific case investigations, money laundering typology sharing is an effective way to foster AML cooperation all over the world.

### 6.3 Implementation, Regulation and Law Enforcement

On the premise of the same standards and effective cooperation, implementation is undoubtedly the last piece of the jigsaw puzzle. To ensure implementation and compliance by all participants in the debit card industry, regulation and law enforcement are indispensable.

There are two levels of regulation and law enforcement. One is the official regulator and competent authority in different jurisdiction, their main responsibility is to make sure the compliance of regulated unites exert punishment on non-compliance conducts and cooperate with their peers from other jurisdictions. The other level relies on international AML organizations and communities like FATF and FSRBs, the Basel Committee, Wolfsberg Group, etc. If there is a black sheep endangering the integrity of AML implementation and cooperation, such organizations and communities should take the lead to reveal the deficiencies, urge the involved party to correct with time limit, and call other parties to resist and reject the business relationship with it.

### 7 Testing Procedure

How to test the performance of an AML framework is an inevitable need for regulators as well as to all participants in the debit card industry when assessing counterparty risks. Such testing procedures should include technical compliance evaluation and implementation effectiveness assessment, and risk-based approach should be the guideline throughout the testing. The following simplified steps are references when conducting an AML test or audit.

#### 7.1 Set Expectation and Recognize Environment

The first step or preparation in advance of a test or audit procedure should be to establish the context, namely the expected outcome, and the recognition of both the internal as well as the external environment.

The expected outcome can also be interpreted as the purpose and scope of the test. For example, the regulatory requirement could be the only element that matters when the test is conducted by the regulator, but if the test result is for
risk assessment of an overseas counterparty or for understanding the overall AML status of an industry, more elements should be included into consideration and the reference standard may be totally shifted. Thus, different expectations directly leads to different needs of environment recognition, which is exactly a reflection of RBA.

In terms of the external environment, it is a comprehensive conception that at least contains regulatory requirements and standard industry practices. A popular analysis model like PEST can be adopted in this process.

When analyzing political factors, it is essential to understand how the government intervenes in AML and the debit card industry, whether or not the government has, for example, criminalized money laundering and published national AML law; adopted FATF recommendations; specified the requirement of issuing a debit card; etc. For economic factors, knowing economic indexes and industrial data like interest rate, inflation rate, the ingredient of income and so on, can be helpful when evaluating risks related to corruption, tax evasion, international trading, and hot money including dirty money. Some index or data like saving rate, the number of debit cards issued, the total and average transaction amount of debit cards, are directly linked to the usage of debit cards. Social factors like employment rate and crime rate can be referred to anticipate predicate crime of money laundering, consumption custom like payment method can be referred to understand debit card overall cardholder behavior pattern. Technological factors like a currency tracking system, fraud prevention technology like a chip card, tokenization, and bio identification, will affect the money laundering and debit card features, as well as its derived products.

The internal environment on the other hand, means that the general AML condition within a corporation, including the structure arrangement, risk appetite, policy and procedures establishment and AML culture. For example, senior management involvement, AML resources allocation, cross-functional cooperation, staff awareness, etc.

Among all the conditions of the internal environment, the identification of the risk appetite and the inherent risk of money laundering are the most important. In terms of risk appetite, due to the terrifying amount of fines imposed on regulated bodies in recent years, most financial institutions have realized the seriousness of AML compliance and strived to adopt a "de-risking" strategy. But it is still not precise to take for granted that all participants in the debit card industry would have a "zero tolerance" for money laundering risks. One reason is due to the gap of laws and regulatory requirements in different jurisdictions—local cooperation may not be required to follow a more stringent standard of AML.

As for the identification of inherent risk, the analyses methodology of product risk, customer risk and country risk can be equally applied to assessing debit card industry. First, the preceding part of the article introduced features,
transaction types and the money laundering techniques of debit cards, which can be referred to as a foundation of product risk assessment. However, there are more details needed to pay attention to, such as if the debit card supports cross-border transaction, if there is an amount limitation of a single transaction or aggregated transactions, etc. Second, for customer risk, besides the KYC information obtained, the issuer should be aware of the cardholder's occupation so that they may understand if the funds scale attached to the debit card is reasonable, and the transaction pattern matches the profile of the customer with the same occupation. Third, country risk should be the major concern if the purpose of testing or auditing is evaluating counterparty risks. There are many country risk-rating tools and results available, elements like whether or not a country is a FATF or FSRBs member; whether the country is suffering from drug dealing, smuggling or terrorism; corruption perception index of the country, and so on are considered. Such tools and results can be applied after a little customization.

7.2 Evaluate Technical Compliance

The second step of a testing or auditing procedure should be reviewing policy and procedure in detail. Compared to the first step, technical compliance evaluation is easier.

Since the expected outcome has been established through the first step, the main process of this step is to cross-check if an AML framework includes policy and procedure as it should have and all components have been covered (e.g., organization structure, customer identification and acceptance, transaction monitoring and reporting, training, recordkeeping, and auditing).

7.3 Assess Implementation Effectiveness

The third step of a testing or auditing procedure is to check the implementation according to the requirements set by an AML framework.

Basically, the process in this step is about finding proofs. If a customer identification and acceptance program of an issuer describes that the debit card shall not be issued before KYC has completed for the customer, then a sampling investigation should be carried out, investigation must retrieve records of the card issuing time and records of the KYC confirmation time to confirm if this requirement is duly implemented. If a policy claims that the cooperation will conduct AML audit annually, the proof should be last year's audit report as well as a record of improvement.

Besides retrieving the historical record, creating samples for a penetration test is also a good solution. For example, if a transaction monitoring system indicates that transactions larger than $10,000 within the same day by the debit card will trigger an alert for investigation, then batches of transactions that match this criteria should be created or simulated to check if they successfully trigger the alert.
7.4 Define Residual Risk and Propose Improvement Suggestion

The last step of a testing or auditing procedure is to calculate residual risk, expose shortage and provide opinions to help improve.

After the previous three steps, the calculation of residual risk should not be a difficult job. Once residual risk has been worked out, compare it to pre-defined expectations, so that the shortage can be exposed, and then provide a recommendation for correction or improvement.

Strictly speaking, defining residual risk and proposing an improvement suggestion is not the last step because the testing or auditing procedure is not a one-way workflow, but a circle loop. Within this loop, the next step should be to follow up with the practice of improvement, and then another round of the same steps of testing and auditing should be performed.

For example, XYZ bank is very prudent about money laundering risks and now the bank wants to know if its existing AML framework is sufficient and effective to cover money laundering risks since the debit card issued by the bank is used without limitation from overseas terminals and can support online transaction via an international switching network. In this case, the referral standard should be a global AML standard of a debit card. The purpose of the testing and auditing procedure is to validate if XYZ is compliant with such standards. One of the inherent risks is the unlimited card usage in overseas countries and XYZ bank previously had not expanded its business to such countries. The residual risk is that despite XYZ bank has conducted country risk assessment, according to the existing AML framework, it has never assessed the risk raised due to acceptance of its debit card by a counterparty acquirer. The exposed shortage then is that XYZ bank established a business relationship without knowing the counterparty's information. The improvement suggestion is that XYZ should immediately conduct due diligence on the counterparty acquirer and any other potential counterparties before they start to accept debit cards issued by XYZ bank. In the next testing and auditing period, one emphasis should be reviewing whether or not XYZ bank has accomplished this improvement.

8 CONCLUSION

Money laundering is a common threat to all participants in the global financial community and it is sensitive to any vulnerability of the community. Debit card as a fundamental financial instrument plays an important role in funds deposit, transfer and disbursement. The function and presence features of debit card make it a good choice particularly to the cross-border layering and integration of money laundering.

To mitigate layering and integration risks of debit cards, a holistic AML framework in this industry is necessary. There are several essential components to build this framework, such as a common practice and standard
to guide every participant in this industry to build a sound AML framework; close cooperation and information sharing mechanism to assist in suspicious activity/transaction investigation and prevention, particularly when the transaction counterparties are scattered in different jurisdictions; thorough implementation of the standard and mechanism; and steadfast regulation as well as law enforcement to safeguard the achievement. In addition, testing or auditing procedure is critical to continuously finding the shortage and improving the framework.

9 REFERENCE
i. https://en.wikipedia.org/wiki/Bank_card
ii. https://usa.visa.com/about-visa.html
viii. Basel Committee on Banking Supervision, Consultative Document; General guide to account opening; July 2015; page 6
ix. The FATF Recommendations; February 2012, Recommendation 17; page 20