FROM KYC TO KYT

BLOCKCHAIN'S EMERGING ROLE IN THE GLOBAL PAYMENTS SYSTEM

PUBLICATION DATE
November 2016

QUINLAN
&ASSOCIATES

IPR2024-00593
Identitii EX2006

ABOUT THE AUTHORS

BENJAMIN QUINLAN

CEO & MANAGING PARTNER

Benjamin Quinlan is the CEO and Managing Partner of Quinlan & Associates.

Prior to founding Quinlan & Associates, Benjamin was the Head of Strategy for Deutsche Bank AG's Equities business in Asia Pacific and its Investment Bank in Greater China, and sat on a number of the bank's global and regional executive committees. He was also the global strategy lead for several of Deutsche Bank's landmark projects executed out of London and New York.

Prior to Deutsche Bank, Benjamin worked as a Management Consultant at Oliver Wyman. Before joining Oliver Wyman, Benjamin worked at UBS AG in the bank's Asia Pacific Client Coverage and Group Strategy departments. He began his career in M&A and Capital Markets Advisory at PwC in Sydney.

YVETTE KWAN

PARTNER

Yvette Kwan is a Partner at Quinlan & Associates.

Prior to joining Quinlan & Associates, Yvette was the Regional Operating Officer (COO) for UBS AG's Corporate Client Solutions division in Asia Pacific, which included UBS's Investment Banking, Capital Markets and Financing Solutions businesses, including its China onshore securities joint venture.

Before taking up her position as Regional Operating Officer, Yvette was an Executive Director in UBS's Group Strategy and M&A departments in Hong Kong, Zurich, Sydney and Hong Kong. She also worked in the Greater China and Corporate Finance team at Credit Suisse First Boston in Hong Kong. Yvette began her career in Emerging Business Services and Corporate Tax at PwC in Sydney.

IPR2024-00593
Identitii EX2006

CONTENTS

EXECUTIVE SUMMARY 4

SECTION 1 DEVELOPMENTS IN THE GLOBAL PAYMENTS SYSTEM 5

SECTION 2 THE COSTS OF AML COMPLIANCE 14

SECTION 3 PROBLEMS WITH EXISTING AML PROCESSES 18

SECTION 4 BLOCKCHAIN SOLUTIONS 24

SECTION 5 CASE STUDY 33

SECTION 6 HOW CAN WE HELP? 36

EXECUTIVE SUMMARY

Correspondent banking relationships have long been used to facilitate cross-border transactions. They have been particularly important for international payments, as well as a bank's own access to offshore financial systems as a means to source products and services that are unavailable in its home jurisdiction.

While banks have traditionally maintained very broad networks of correspondent banking relationships, there are growing indications that this is changing. In fact, from mid-2011 until the end of 2015, the number of correspondent banking relationships worldwide fell despite global payment volumes rising over the same period. Much of this has been driven by banks cutting relationships in jurisdictions where returns do not justify the costs (and risks) of investment. While some of this 'trimming' reflects a broader deleveraging by many banks following the global financial crisis, the most common driver of reduced profitability has been the increased cost of regulatory compliance, particularly with respect to Anti-Money Laundering (AML)/Counter Terrorism Financing (CTF) (together, AML) regulations.

The quantum of AML compliance costs for the banking industry is far from trivial. Banks globally are forecast to spend an estimated USD 12 billion on their AML compliance programs in 2016. A further USD 16 billion in fines were handed out by U.S. regulators alone since the end of 2009 for AML compliance failings. Many institutions have responded by offboarding more risky customers as part of a general 'de-risking' strategy, which is posing a very real risk to the workings of the global financial system. We believe this is a trend that must be reversed.

The core problem with existing AML compliance processes at most banks is that they are extremely labour-intensive, with over three-quarters of bank compliance budgets dedicated to personnel responsible for manually onboarding new clients (i.e. KYC or Know Your Customer processes), investigating suspicious payment activities (i.e. surveillance) and producing internal and external reports (i.e. reporting). Moreover, current payment messaging systems such as Society for Worldwide Interbank Financial Telecommunication (SWIFT) are in need of an overhaul, given limited information capture, a lack of straight-through-processing, and the capacity for information to be altered, incorrect or even missing.

We believe blockchain technology will have an increasingly important role to play in enhancing the global payments system, both in terms of reducing the amount of manual labour involved with existing AML compliance processes, as well as optimising legacy technology systems that are in operation today. In particular, we see huge potential in the immediate-term for it to run alongside legacy payment and messaging infrastructure, overlaying existing systems with a rich information layer.

We estimate blockchain technology has the potential to deliver the industry USD 4.6 billion in annual AML cost savings (i.e. 32% of current annual costs) in the form of (1) reduced compliance headcount and associated costs (2) lower technology spend and (3) fewer regulatory penalties. However, in order for any of these blockchain solutions to truly work, industry-wide adoption is needed. Only then will banks be in a position to move from KYC to KYT i.e. a 'know your customer' approach to AML to a 'know your transaction' solution.

IPR2024-00593
Identitii EX2006

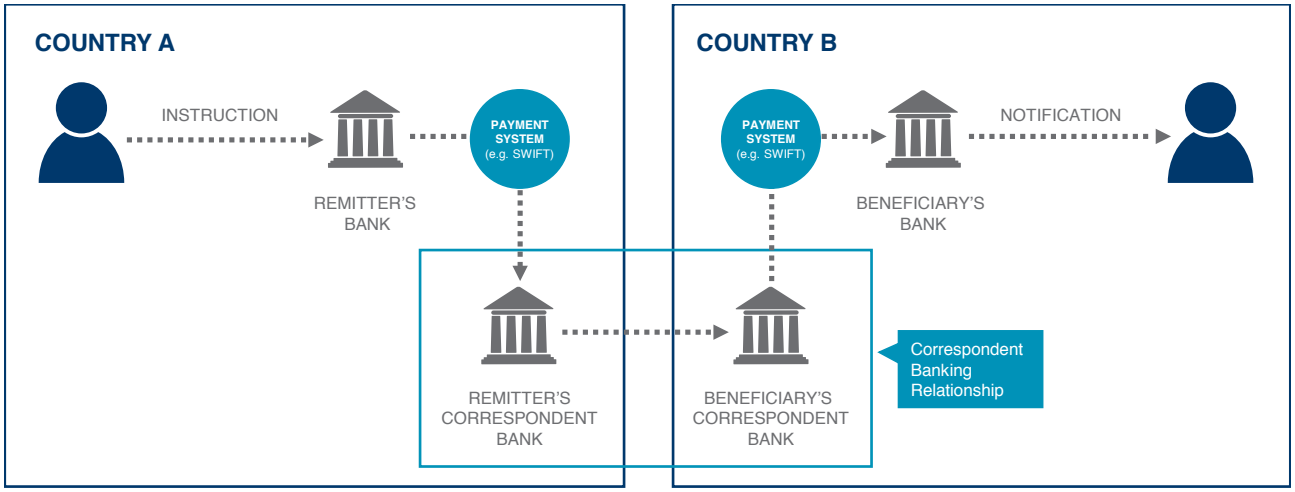
SECTION 1
DEVELOPMENTS IN THE GLOBAL PAYMENTS SYSTEM

WHAT IS CORRESPONDENT BANKING?

In its simplest form, correspondent banking involves 'agreements or contractual relationships between banks to provide payment services for each other.'[1] Typically, this will involve 'an arrangement under which one bank (correspondent) holds deposits owned by other banks (remitters/beneficiaries) and provides payment and other services to those remitter/beneficiary banks.'[2]

Correspondent banking relationships are often reciprocal, with institutions providing services to one another, normally in different currencies (see Figure 1). These services may include international funds transfers, cash management services, cheque clearing, loans and letters of credit, as well as foreign exchange.

FIGURE 1: CORRESPONDENT BANKING PAYMENT FLOWS (ILLUSTRATIVE)



Source: Quinlan & Associates analysis

1 ECB, 'Ninth Survey on Correspondent Banking in Euro,' February 2015,available at: www.ecb.europa.eu/pub/pdf/other/surveycorrespondentbankingineuro201502.en.pdf

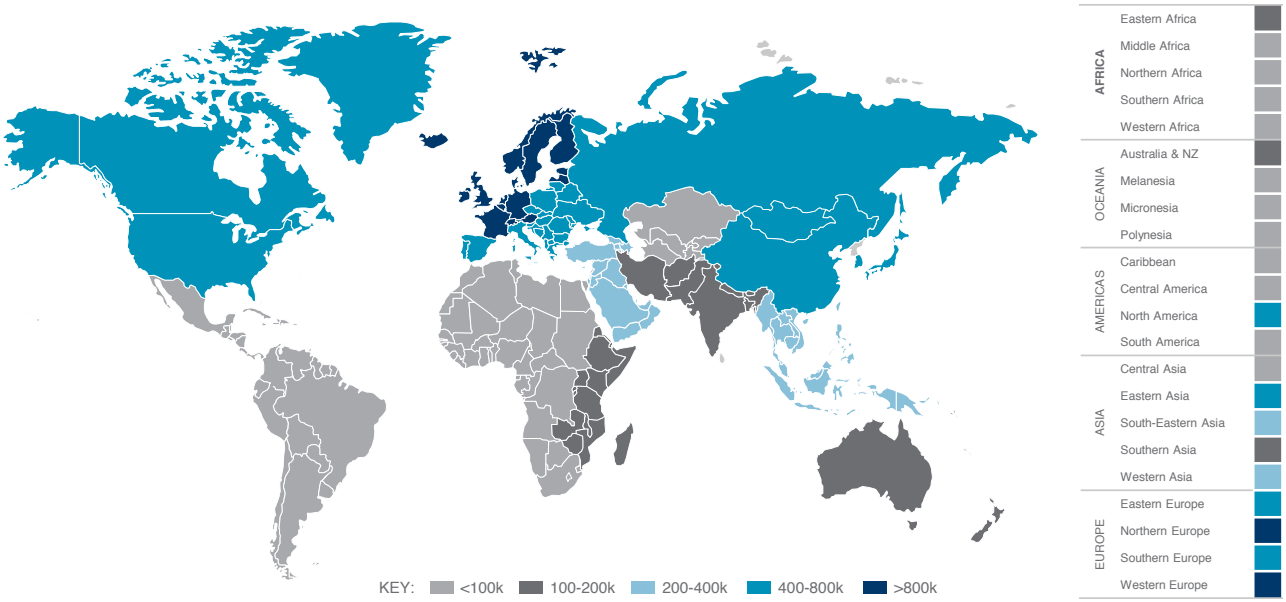
2 CPMI, 'A Glossary of Terms Used in Payments and Settlement Systems,' March 2003 (updated June 2015), available at: www.bis.org/cpmi/publ/d00b.htm?m=3%7C16%7C266

IPR2024-00593
Identitii EX2006

While financial market infrastructures have reduced the importance of correspondent banking relationships for domestic payments in a single jurisdiction, they remain critical for cross-border transactions. This is especially the case for international customer payments, as well as a bank's own access to offshore financial systems – namely, to source services and products that may not be available in its own jurisdiction.

The most active correspondents across all corridors (by region) include banks in Northern and Western Europe. Other active regions include Eastern and Southern Europe, Eastern Asia, and North America. According to the Bank for International Settlements (BIS), payment traffic is most concentrated within the triangle linking Europe (ex Eastern Europe) with Asia and North America. The least active correspondent banks are located in developing markets, including Africa, Latin America and Central Asia (see Figure 2).

FIGURE 2: ACTIVE CORRESPONDENT RELATIONSHIPS (PER REGION)



Note: Continents and regions grouped according to the United Nations Statistics Division; data based on monthly averages

Source: SWIFT Watch, BIS, Quinlan & Associates analysis

IPR2024-00593
Identitii EX2006

RECENT TRENDS

Recognising the considerable interest central banks have in international trade and cross-border payments, the BIS published a detailed report in July 2016 which looked at recent developments in the global correspondent banking industry.[3] The report outlined a number of key trends explored below.

FEWER RELATIONSHIPS

According to the BIS, while banks have traditionally maintained very broad networks of correspondent banking relationships, there are signs this might be changing.

Specifically, the BIS found that some banks providing these services 'are reducing the number of relationships they maintain and are establishing few new ones.'

Data from Deutsche Bundesbank and SWIFT confirms these findings: while global correspondent banking volumes increased from mid-2011 to December 2015, the number of active correspondent banks declined over the same period (see Figure 3).

This trend is most pronounced for remitter/beneficiary banks that:

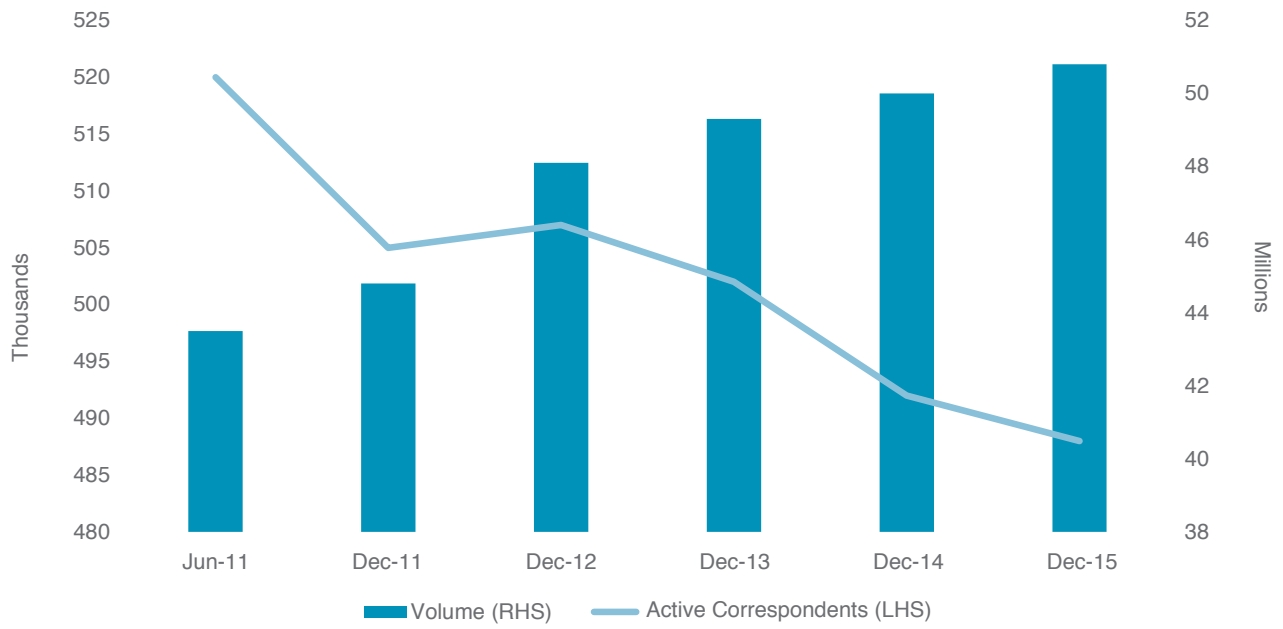
1. Lack sufficient volumes to recover compliance costs;
2. Are located in 'risky' jurisdictions;
3. Lack adequate risk assessment capabilities; or
4. Offer products or services or have customers that pose a higher risk for AML.

These results are supported by a World Bank survey at the end of 2015, which found that 75% of large international banks have seen a decline in their number of Vostro accounts. For local and regional banks, 60% have experienced a decline in their number of correspondent banking relationships (see Figure 4).

3 BIS, 'Correspondent Banking,' July 2016, available at: http://www.bis.org/cpmi/publ/d147.pdf

IPR2024-00593
Identitii EX2006

FIGURE 3: NUMBER OF ACTIVE CORRESPONDENTS (ALL CORRIDORS)

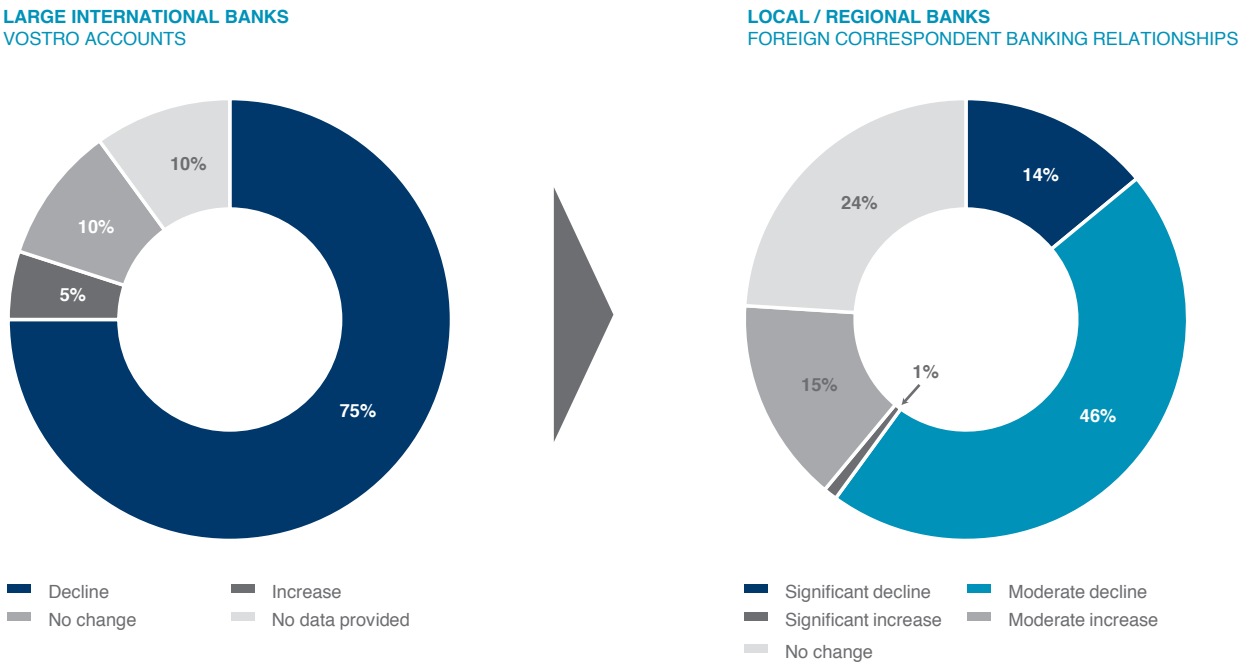


Note: Data is based on 3-month moving averages

Source: Deutsche Bundesbank, SWIFT Watch, BIS, Quinlan & Associates analysis

IPR2024-00593
Identitii EX2006

FIGURE 4: TRENDS IN CORRESPONDENT BANKING RELATIONSHIPS



Source: World Bank

CHANGING RELATIONSHIPS

Correspondent banking services which are perceived to have higher associated risks (such as nested correspondent banking and payable-through accounts) have been scaled back in favour of more traditional services. These traditional relationships are often retained to support corporate customers' cross-border payments and trade finance activities, facilitate the cross-selling of other products to remitter/beneficiary banks, or preserve reciprocity in correspondent relationships.

CONCENTRATED RELATIONSHIPS

Fewer correspondent banking relationships, coupled with changes in the nature of those relationships, have led to a high concentration of relationships in a relatively small number of institutions. This has led to greater market dominance by the largest correspondent banking players. The BIS also observed a concentration of correspondent banking activities within affiliated banks. For multi-currency financial market infrastructure (FMIs), the reduction in the number of correspondent banking relationships has also reduced the number of backup correspondent options.

IPR2024-00593
Identitii EX2006

RISING COSTS

The set-up and ongoing management of correspondent banking relationships is becoming more difficult for both correspondent and remitter/beneficiary banks, given rising costs. While some of this reflects higher capital and liquidity costs facing banks more generally, the vast majority of this is being driven by a surge in AML/CTF compliance costs.

CUTBACKS IN SPECIFIC CURRENCIES

A number of players are reluctant to provide correspondent banking services in specific foreign currencies, especially where the perceived risks of economic sanctions, regulatory burdens related to AML/CTF, as well as implementation uncertainties and reputational risks associated with non-compliance, are higher. BIS research also suggests that correspondent banking activities in US dollars are increasingly concentrated in US banks, while non-US correspondent banks are focusing their activities in their domestic currency.

GEOGRAPHIC IMBALANCES

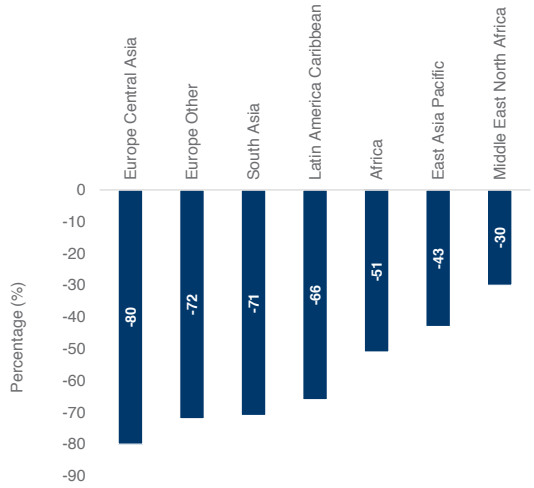
The impact of these trends is being felt to different degrees across various jurisdictions. In particular, smaller remitter/beneficiary banks located in more 'risky' jurisdictions have been impacted most by the reduction in the number of relationships. Data from the World Bank indicates that local/regional banks in emerging market jurisdictions have been hit hardest, including those in Europe Central Asia, as well as South Asia, Latin America and Africa. The majority of terminations or restrictions on correspondent banking relationships is coming from banks located in developed markets, especially the U.S. (see Figure 5).

With many remitter/beneficiary banks in danger of being cut off from international payment networks, the BIS found a growing risk that cross-border payment networks might fragment, narrowing the range of options available for such types of transactions.

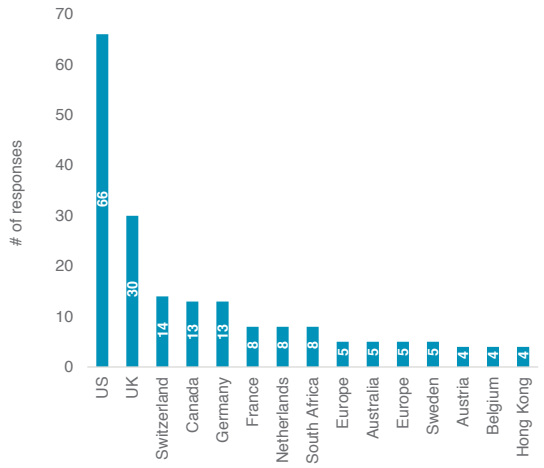
IPR2024-00593
Identitii EX2006

FIGURE 5: GEOGRAPHIC TRENDS IN RELATIONSHIPS

LOCAL/REGIONAL BANKS
DECLINE IN CORRESPONDENT BANKING RELATIONSHIPS (BY REGION)



LOCAL/REGIONAL BANKS
TERMINATION AND RESTRICTIONS OF CORRESPONDENT BANKING RELATIONSHIPS (BY INITIATING BANK NATIONALITY)



Source: World Bank

IPR2024-00593
Identitii EX2006

DRIVERS

The BIS found the reduction in the number of global correspondent banking relationships was being driven by a mix of factors from the demand-side (i.e. remitter/beneficiary banks) and the supply-side (i.e. correspondent banks) (see Figure 6).

While the BIS recognised some of these trends were being spurred by remitter/beneficiary banks, it found significant demand for these services continues to exist. In its view, the key driver of the reduction in the number of global correspondent banking relationships is the supply-side (i.e. the correspondent banks themselves), who have been cutting customers and/or jurisdictions where returns do not justify the costs (and risks) of investment.

FIGURE 6: DRIVERS OF RECENT TRENDS

DEMAND DRIVERS
REMITTER/BENEFICIARY BANKS

- ✓ Reduce risk management work
- ✓ Simplify reporting of intraday liquidity
- ✓ Concentrate payment channels
- ✓ Minimise costs

SUPPLY DRIVERS
CORRESPONDENT BANKS

- ✓ Reduce rising capital & liquidity costs
- ✓ Cut unprofitable customers/jurisdictions
- ✓ Minimise surging AML/CTF costs
- ✓ Lower risk of fines/reputational damage

Source: BIS, Quinlan & Associates analysis

IPR2024-00593
Identitii EX2006

While some of this 'trimming' reflects a general deleveraging by many banks following the global financial crisis, the most common driver of reduced profitability has been the increased cost of regulatory compliance, particularly with respect to AML/CTF regulations. Correspondent banks have also become extremely sensitive to the risk of potential fines – and any associated reputational damage – from non-compliance. In a survey of large international banks conducted by the IMF, the top two reasons driving the reduction in correspondent banking relationships were concerns about money laundering/terrorism financing and the imposition of international sanctions, cited by 95% and 90% of respondents respectively.[4]

The correspondent banking business is, at its core, one that relies heavily upon economies of scale. However, it is becoming increasingly clear that volumes in certain jurisdictions and/or with certain customers do not justify the burgeoning AML/CTF compliance costs involved for many players, leading to a reduction in correspondent relationships. Such trends are putting the entire global payments system at increased risk of fragmentation.

"...THE MOST COMMON DRIVER OF REDUCED PROFITABILITY HAS BEEN THE INCREASED COST OF REGULATORY COMPLIANCE, PARTICULARLY WITH RESPECT TO AML/CTF REGULATIONS."

4 The World Bank, 'Withdrawal from Correspondent Banking: Where, Why and What to Do About it?,' November 2015, available at: http://documents.worldbank.org/curated/en/113021467990964789/pdf/101098-revised-PUBLIC-CBR-Report-November-2015.pdf

IPR2024-00593
Identitii EX2006

SECTION 2
THE COSTS OF AML COMPLIANCE

'Money laundering and the financing of terrorism are financial crimes with economic effects. They can threaten the stability of a country's financial sector or its external stability more generally. Effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse. Action to prevent and combat money laundering and terrorist financing thus responds not only to a moral imperative, but also to an economic need.' [5]

Min Zhu
Deputy Managing Director, IMF

Money laundering – including the financing of terrorism – poses a considerable threat to the stability of the global financial system and broader economy, given its capacity to impact the integrity of financial institutions, distort international capital flows and deter foreign investment activity.

Money launderers and terrorist financiers capitalise on the inherent complexity of the financial system and differences in national AML/CTF laws, and have been particularly active in targeting jurisdictions where AML/CTF controls are weakest. The problem has become so large that the United Nations estimates that between USD 800 billion to USD 2 trillion is laundered each year, representing 2-5% of global GDP. However, less than 1% of illicit financial flows globally are seized by authorities.[6]

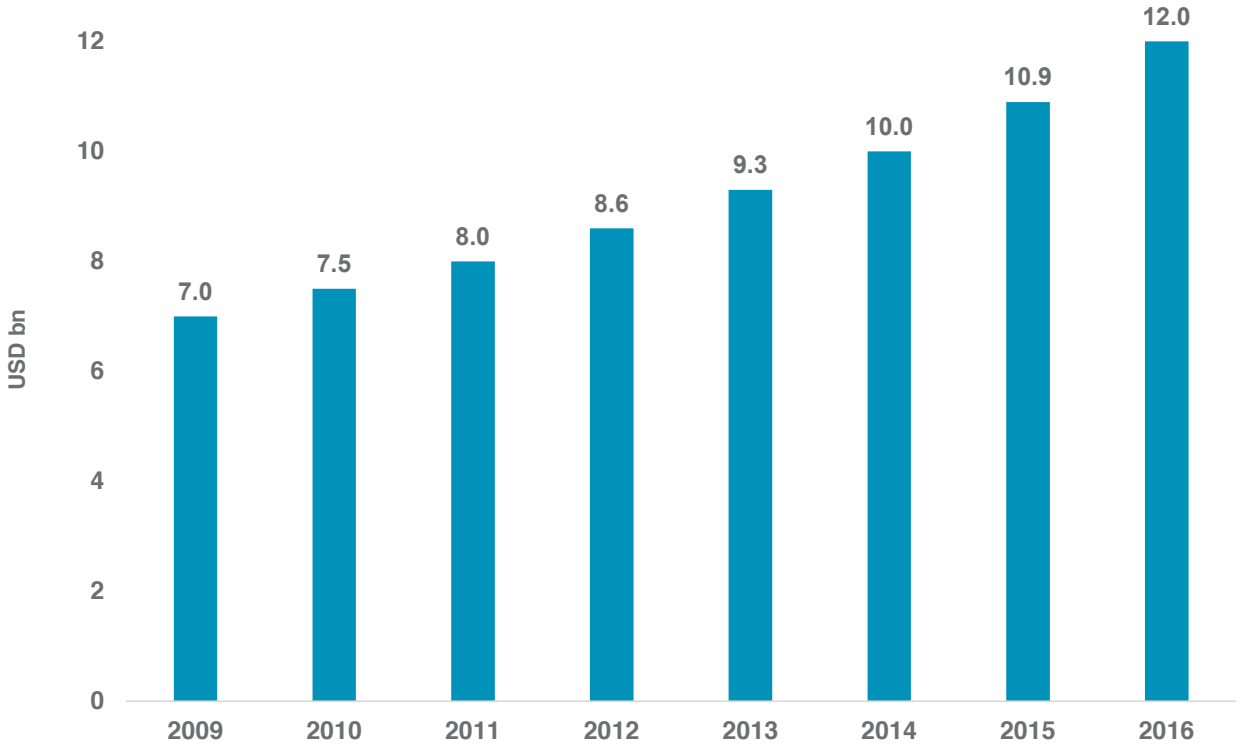
Given the importance of AML/CTF regulations in enhancing both the stability and integrity of the financial sector, global regulators have developed extensive guidelines for banks' internal AML programs. In order to adhere to these guidelines, banks have made substantial investments in their in-house AML compliance capabilities. In fact, global AML compliance spend is expected to top USD 12 billion by the end of 2016, up by over 70% from USD 7 billion in 2009 (see Figure 7).

5 IMF Factsheet, The IMF and the Fight Against Money Laundering and the Financing of Terrorism, March 2016, available at: http://www.imf.org/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism?pdf=1

6 United Nations Office on Drugs and Crime website, available at https://www.unodc.org/unodc/en/money-laundering/globalization.html

IPR2024-00593
Identitii EX2006

FIGURE 7: GLOBAL AML COMPLIANCE COSTS



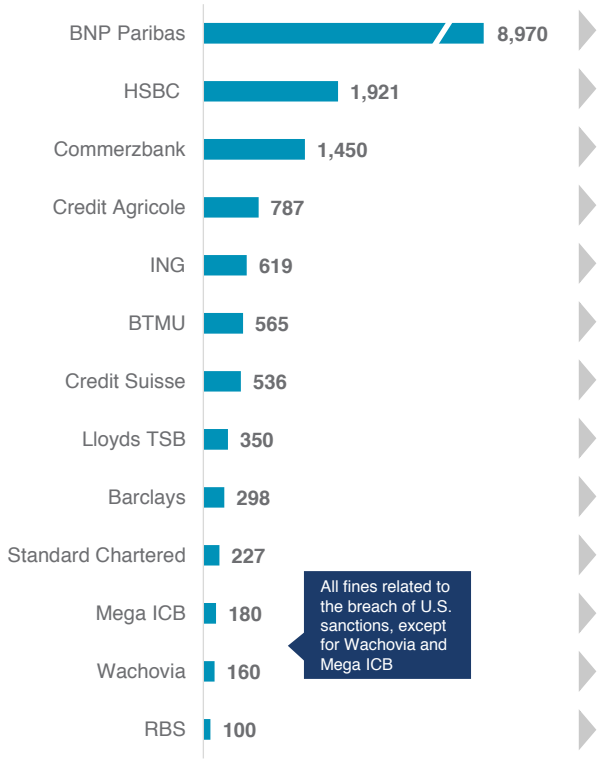
Source: Accenture, Celent, Quinlan & Associates estimates

Notwithstanding the efforts banks have made to detect and eliminate money laundering, our discussions with a number of senior AML compliance specialists indicates that only 1-2% of all money laundering activity is actually detected, which has resulted in banks being slapped with sizeable regulatory penalties. Various AML compliance failings include weak governance processes, ineffective AML policies, and/or poor monitoring and reporting procedures.

Since 2009, U.S. regulators alone handed out over USD 16 billion in AML-related penalties to 13 banks for separate compliance failings, the majority of which related to sanction breaches (see Figure 8). The largest individual fine was USD 8.97 billion, handed out to BNP Paribas for processing USD 9 billion of transactions involving Iran, Sudan and Cuba. HSBC and Commerzbank also paid fines of USD 1.92 billion and USD 1.45 billion respectively for conducting transactions on behalf of customers in sanctioned countries. HSBC was also alleged to have helped launder USD 881million in drug proceeds through the U.S. financial system.

IPR2024-00593
Identitii EX2006

FIGURE 8: LARGEST U.S. AML-RELATED FINES (USD 100m+)



DATE	DESCRIPTION
Jun 2014	• Processed USD 9bn in transactions from 2004-12 for Sudan, Iran & Cuba
Dec 2012	• Processed transactions for Cuba, Iran & Libya and laundered USD 881m in drug proceeds
Mar 2015	• Processed transactions with a number of Iranian and Sudanese entities
Oct 2015	• Processed USD 32bn in payments on behalf of Sudanese, Iranian, Burmese and Cuban entities
Jun 2012	• Moved USD 2bn worth of transactions on behalf of Cuban and Iranian entities
Nov 2014	• Watered down a report on the bank's dealings with Iran, Myanmar and Sudan
Dec 2009	• Engaged in transactions on behalf of customers from Iran and Sudan
Jan 2009	• Engaged with Iranian customers, who processed USD 350m through U.S. correspondents banks
Aug 2010	• Stripped wire transfers for customers in Cuba, Iran and various other countries
Dec 2012	• Removed information from wire transfers for customers in Iran, Sudan, Libya and Burma
Aug 2016	• Failed to report suspect transactions and displayed indifference towards risks of transactions with Panama
Mar 2010	• Laundered USD 100m in illegal drug proceeds for Mexican drug cartels
Dec 2013	• Engaged in transactions with entities in Iran, Sudan, Cuba and Burma

Note: HSBC figure includes USD 665 million in civil penalties to the Office of the Comptroller of the Currency, the Federal Reserve, and the Treasury Department; BTMU figure includes USD 250m paid in June 2013 for carrying out transactions with sanctioned countries, as well as an additional USD 315m in November 2014 for pressuring consultants to move key information about those transactions; RBS's fine represents its settlement sum with U.S. regulators; BNP numbers represent USD 140 trillion in fines and USD 8.83 billion in forfeitures

Source: Press releases, Quinlan & Associates analysis

IPR2024-00593
Identitii EX2006

One of the most recent cases occurred in August 2016 when the Department of Financial Services, New York's financial regulator, imposed a USD 180 million fine on Taiwan's Mega International Commercial Bank for AML failures, which included having links to the law firm at the centre of the Panama Papers scandal.[7] As a result of this incident, the bank's Chairman stepped down.

With AML compliance costs skyrocketing and AML-related penalties on the rise, the global banking industry has been grappling with how to manage not just their correspondent banking relationships, but also their own client base. For example, while Deutsche Bank committed to further developing its Know Your Customer (KYC) and AML infrastructure as part of its 'Strategy 2020' announcement, it also plans to offboard up to 50% of its clients in its Global Markets (GM) & Corporate & Investment Banking (CIB) units.[8] This is because 'tail' accounts, which represent 70% of the GM & CIB client base, generate only 20% of total GM & CIB revenues. Notwithstanding this, they still incur fixed onboarding costs which can often be comparable to much larger accounts.

Similar offboarding strategies are being adopted by many global banking players across multiple business lines. We believe this ongoing trend of 'de-risking' poses a considerable threat to the workings of the global financial system, including the ability for smaller firms to secure the relevant banking services they need to grow (e.g. funding, hedging, advisory). Without knowing it, banks are inadvertently creating competitive distortions by further entrenching the dominance of larger firms within their respective industries. We believe this is a trend that must be reversed.

7 Wall Street Journal, 'Bank Fined for AML Failures, Panama Papers Links,' 22 August 2015, available at: http://blogs.wsj.com/riskandcompliance/2016/08/22/new-york-regulator-fines-taiwanese-bank-180m/

8 Deutsche Bank, 'Executing Strategy 2020,' 29 October 2015, available at: https://www.db.com/ir/en/download/Deutsche_Bank_Strategy_2020_29_October_2015.pdf

IPR2024-00593
Identitii EX2006

SECTION 3
PROBLEMS WITH EXISTING AML PROCESSES

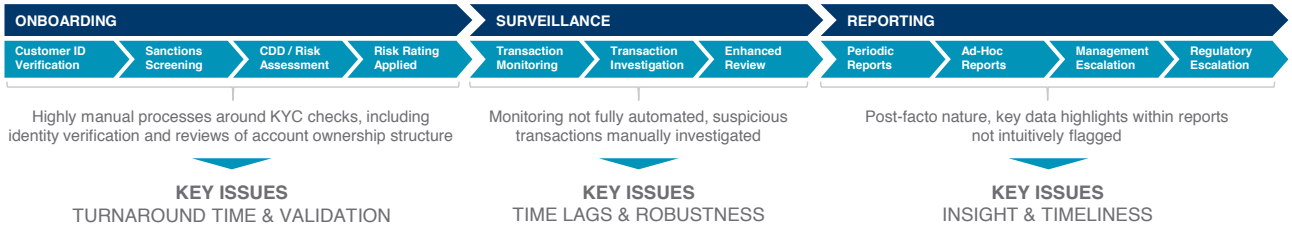
There are two underlying problems with existing AML compliance processes at most banks, namely: (1) manual processes; and (2) legacy technology.

1. MANUAL PROCESSES

The core problem with AML compliance processes at most banks is the fact that they are extremely labour-intensive. While we understand some parts of the AML process are automated, the majority of bank compliance budgets are dedicated to personnel responsible for manually onboarding new clients (i.e. KYC) and investigating suspicious payment activities (i.e. surveillance).

As it stands, manual input is required across all key stages of the AML compliance process, including (A) onboarding, (B) surveillance and (C) reporting (see Figure 9). We will discuss each of these in detail below.

FIGURE 9: AML COMPLIANCE PROCESS



Source: Industry interviews, Quinlan & Associates analysis

IPR2024-00593
Identitii EX2006

A. ONBOARDING

When a client looks to open a new account, banks will engage in exhaustive KYC checks, comprising customer identification verification (in which banks will also look at the beneficial ownership of accounts), sanctions screening and customer risk assessments, including detailed documentation reviews. These checks are highly labour-intensive, given the inherent complexity of many corporate and institutional ownership structures.

Even for automated client background screening searches, our discussions with compliance professionals indicates that more than 80% of KYC alerts are false alarms. This can rise to as high as 99% in countries like China, due to issues with language translation and significant duplicity with individual names, given the country's vast population size. However, each of these alerts (including false alarms) needs to be manually reviewed by KYC officers, which takes up significant amounts of manpower.

Manual processes have a considerable impact on turnaround times. A regional head of business management we interviewed at a leading global wealth manager said the average turnaround time to onboard a private banking client was two to three weeks. For more complex clients such as trusts or corporates with mutiple layers of beneficial ownership, average onboarding times were one to three months and, in some cases, much longer. These KYC checks are also highly duplicative in nature: banks in many jurisdictions are required to conduct independent KYC checks on prospective accounts, even when the account has been comprehensively vetted by another bank. This duplication of effort also occurs to a great extent within a single firm, with banks maintaining highly duplicative KYC processes for onboarding the same client across different departments and jurisdictions.

Morgan Stanley's recent decision to not submit a proposal for the upcoming IPO of China's Anbang Insurance in mid-2017 due to questions around the firm's ownership structure provides a clear indication of just how serious banks are in adhering to KYC compliance standards. In effect, the risks are perceived to be so large that the U.S. bank is prepared to step away from what could potentially be one of the biggest IPOs in 2017.

IPR2024-00593
Identitii EX2006

B. SURVEILLANCE

Once onboarded, many banks use intelligent software tools to monitor their clients' transactions, such as remittances, investment activities and loan/deposit rollovers. This is done on both a pre-transaction real-time basis (e.g. sanctions screening) and post-transaction periodic, remedial basis (e.g. suspicious activity). Any transactions that give rise to an alert are manually investigated by a bank's compliance team.

Our discussions with a number of compliance professionals at global investment banks indicates that between 5-10% of transactions are alerted for potential suspicious activity, with 99.9% of cases delivering a false positive result. Even so, compliance/risk management officers are still required to manually follow up on these cases, which again consumes a significant amount of time.

Moreover, the vast majority of these false positives are not due to weaknesses in monitoring software but are largely a reflection of the poor quality of transaction data, such as the absence of sender identification details. As a result, a manual reconciliation process is required to check information that is syntactically misrepresented or incomplete.

C. REPORTING

Our interviews with a number of AML professionals at global banks indicates that more than 90% of management reports are automatically generated, either in-house or through an outsourced provider. These 'downstream' reports typically provide information to a bank's senior management on total account openings, beneficial owners, client domiciles, and any violations or compliance breaches for a defined period of time.

Banks also produce periodic surveillance reports, such as suspicious activity reports or transaction activity reports. However, they are often prepared on a post-facto basis. As such, when a compliance breach is identified, it is often too late to remediate. Moreover, key data focus areas within these reports are not intuitively flagged for the reader, such that a large amount of manual time is needed to review them.

In addition to producing periodic AML reports, banks are required to maintain all records of all their clients' transactions, including client due diligence records, to comply with ad-hoc regulatory requests and self-identified escalations. According to recommendations laid out by the Financial Action Task Force (on Money Laundering) (FATF) in June 2016, 'financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any).'[9]

Some of these regulatory requests can be highly non-standardised, requiring a great degree of manual effort to produce bespoke reports. We also found tracking processes to be problematic, with most banks unable to determine how many resources are needed to open a single account, given the process can be very complex and involve a number of different parties. As such, the underlying cost of onboarding a new account is extremely difficult to quantify.

9 FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,' February 2012 (updated June 2012), available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

IPR2024-00593
Identitii EX2006

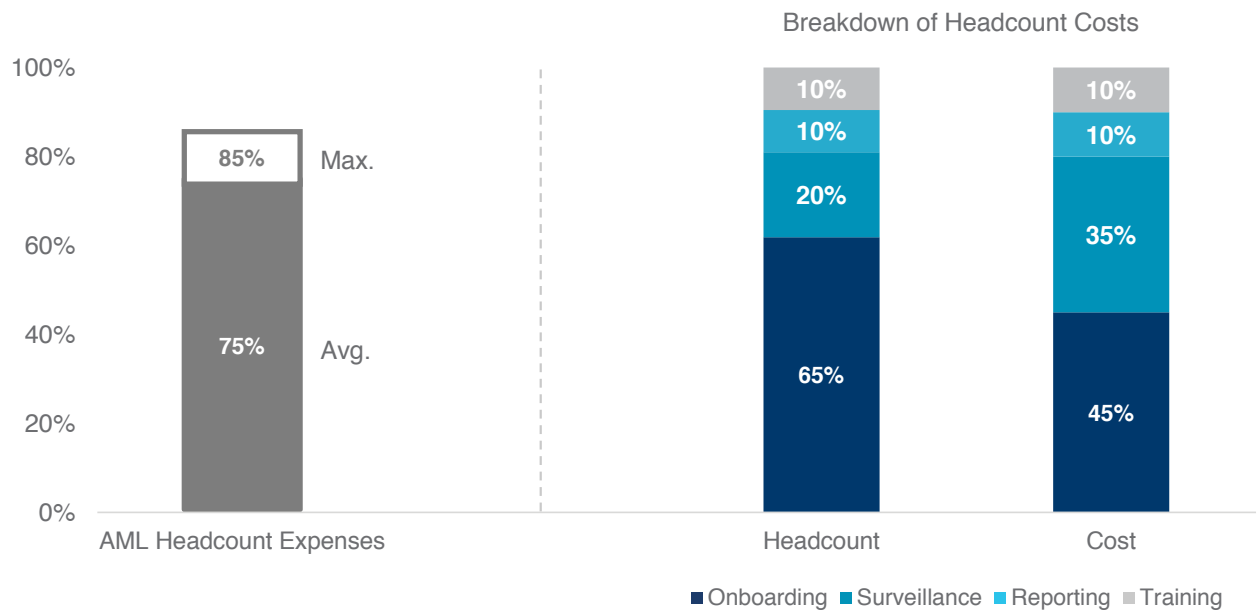
HEADCOUNT COSTS

Our research indicates that headcount costs represent anywhere between 75-85% of total AML-related compliance spend, with the remainder devoted to technology.

For the global banks we spoke to (including international corporate and investment banks), onboarding was estimated to account for 65% of AML-related compliance headcount and 45% of headcount costs (see Figure 10).[10] We also found banks are dedicating increasingly more resources to the cause.

A senior compliance professional at one global bank we interviewed said they had recently submitted a hiring request for a dozen additional full-time employees to remediate onboarding issues for more than 1,000 existing accounts in their Asia Pacific business unit by the end of 2018.

FIGURE 10: BANK AML COMPLIANCE SPEND STRUCTURES – HEADCOUNT



Source: Quinlan & Associates proprietary analysis, based on discussions with senior compliance, onboarding and surveillance professionals at five global banks

10 Note that onboarding employees are relatively inexpensive when compared to other compliance professionals

IPR2024-00593
Identitii EX2006

Surveillance employees are estimated to account for 20% of AML-related compliance headcount and 35% of costs, given the expertise is quite niche (and therefore relatively expensive). Most surveillance staff, however, are focused on identifying insider trading and market manipulation activities, though banks have been aggressively expanding their AML surveillance teams, especially in private and transaction banking.

Training represents 10% of total compliance headcount and costs, though a move to developing online employee compliance training modules has seen these costs increasingly migrate to IT spend. Reporting also accounts for 10% of compliance headcount and costs, given much of it is automated.

2. LEGACY TECHNOLOGY

Current regulations require banks to adhere to KYC, sanctions and AML compliance standards at the transaction level. For example, the U.S. Office of Foreign Assets Control (OFAC) regulations require screening transactions for possible sanction violations, with such obligations even applying to a correspondent bank. The challenge that correspondent banks face is that the remitter and beneficiary of a transfer may not be clients of the correspondent bank, leading to onerous and duplicative KYC efforts. As a result, many players are walking away from correspondent banking activities.

In Europe, the regulatory requirements of EU Funds Transfer Regulation 2015 will apply for transactions into or through the European Economic Area from 26 June 2017. Further requirements on correspondent banks and other intermediary payment service providers include the transmission of additional information on the beneficiary, including beneficial ownership and whether they are a politically exposed person (PEP). It also sets higher standards and obligations on such providers to detect insufficient or missing data.

SWIFT provides one of the largest worldwide financial messaging systems for financial institutions to send and receive information to support global payment orders. Its key characteristics are standardised messaging and a relatively secure network. The historical success of SWIFT (and other comparable messaging systems) can largely be attributed to its ability to talk to the various different operating systems of intermediaries across the payments process.

IPR2024-00593
Identitii EX2006

Notwithstanding the widespread adoption of messaging systems such as SWIFT, we see a number of limitations associated with the current global payments infrastructure, especially in light of ongoing regulatory developments around AML/CTF:

1. **Limited information capture:** while the industry is embracing the ISO20022 XML messaging standard, SWIFT's current 'MT' messaging format (e.g. MT103) limits the amount of information that can be sent between banks, given the original messaging system was not designed to cater to much larger bandwidths needed for richer underlying data sets.
2. **Lack of interoperability between banks' back-end systems:** the lack of standardisation in banks' back-end operating systems means that the much richer data set required to comply with increasing AML regulations cannot be effectively shared between banks.
3. **Parties are difficult to identify:** other than the remitter and beneficiary's own banks (i.e. the banks that have the direct, onboarded relationships), other banks along the correspondent banking value chain may not know the true identity of the transacting parties, including any ultimate benefifcial owners. However, they are still required to comply with KYC, CTF and AML regulations.
4. **No straight-through-processing (STP):** pre-transaction checks require manual review of information against a bank's own data sets (e.g. sanction and PEP lists), inhibiting the ability to conduct straight-through-processing (STP). These manual processes result in considerable time delays for international money transfers.
5. **Capacity for information to be altered/ incorrect/missing:** payments can still be processed when information contained within the payment instruction is missing, incorrect or even altered. The ability to forge SWIFT messages saw Bangladesh's central bank hacked for USD 81 million in early 2016.[11]
6. **Time-limited information capture:** SWIFT only stores messages for a period of 180 days. Given banks are required by regulators to store transaction data for a period of up to five years, they must rely on their own data storage and retrieval systems.

In the next part of this report we will examine the emerging role of blockchain technology in the global payments system.

11 Recognising some of the limitations in its technology, SWIFT has announced that, starting in December 2016, it would begin sending 'Daily Validation Reports' to clients. These reports would list messages sent from the client's SWIFT terminal, allowing banks to spot payment instructions they did not intend to send. These will be supplemented by a risk report, intended to spot anomalies in a bank's normal pattern of money transfers.

IPR2024-00593
Identitii EX2006

SECTION 4
BLOCKCHAIN SOLUTIONS

We believe blockchain technology will have an increasingly important role to play in enhancing the global payments system. In particular, it offers considerable potential to reduce the amount of manual labour involved with existing AML compliance processes, as well as optimise many legacy technology systems that are currently in operation today.

BLOCKCHAIN OVERVIEW

In its simplest form, blockchain is a type of distributed ledger database that records and maintains a constantly growing list of transactions into sequential blocks. No centralised party, such as a clearinghouse, validates and executes transactions; instead, a network of computers, which serve as interconnected 'nodes' within the network, maintains and verifies a record of consensus of those transactions.[12]

The transactions are then encrypted and stored in linked blocks on the nodes, creating a cryptographic audit trail. These blocks are immutable and can't be changed or deleted. As a result, all nodes in the network have access to a shared, single source of truth (see Figure 11).

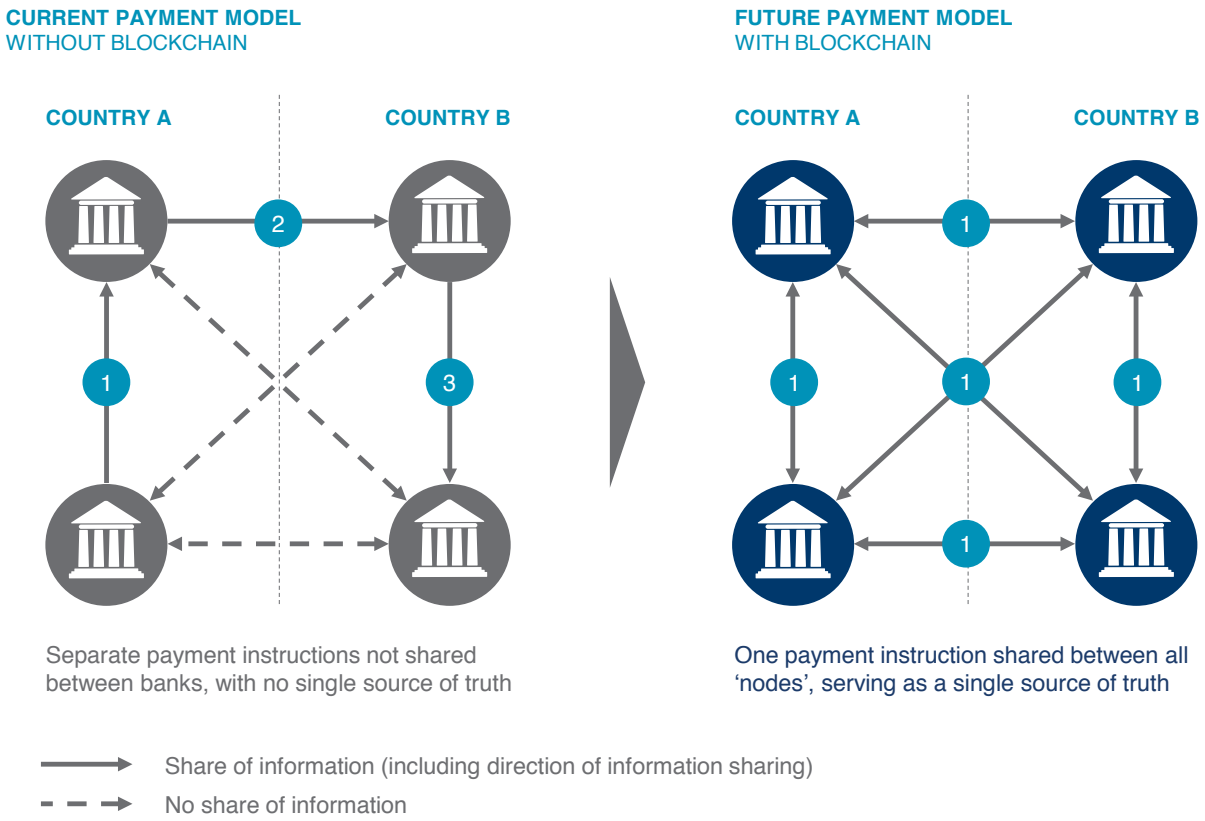
BLOCKCHAIN AND GLOBAL PAYMENTS

We believe blockchain technology has significant scope to improve the current global payments system. We can identify a number of key benefits from the perspective of both the customers and the institutions that service them (see Figure 12).

12 A consensus mechanism is a method of authenticating and validating a transaction on a blockchain, such as a pre-agreed set of rules. Such a mechanism is critical to the effective operation of any distributed ledger.

IPR2024-00593
Identitii EX2006

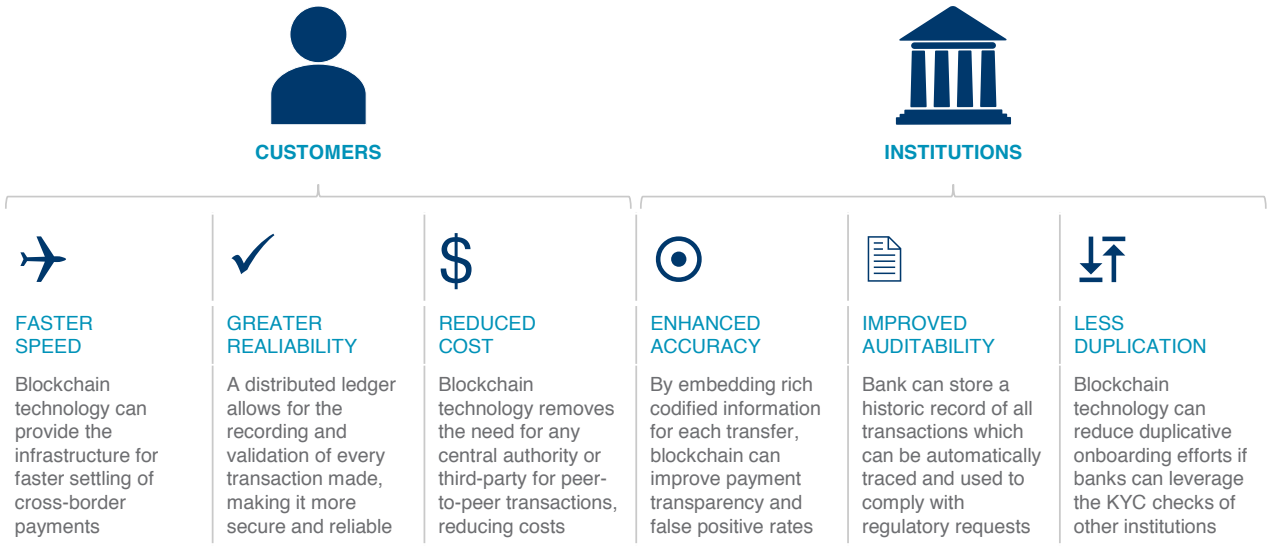
FIGURE 11: ILLUSTRATIVE REMITTANCE PROCESS



Source: Quinlan & Associates proprietary analysis

IPR2024-00593
Identitii EX2006

FIGURE 12: BENEFITS OF BLOCKCHAIN



Source: Quinlan & Associates proprietary analysis

While we believe blockchain technology may ultimately result in a reduced need to use correspondent banking relationships for cross-border transactions, we see huge potential in the immediate-term for it to run alongside – and hence modernise – legacy payment and messaging infrastructure, overlaying existing systems with a rich information layer.

We feel there is particular scope for value to be added at the transaction level. This is because, in the current environment, it is difficult for banks to conduct risk-based analysis of individual payments: instead, bank surveillance teams (and the software that supports them) tend to focus their efforts on monitoring overall transaction patterns. Suspicious activity is typically only identified when an abnormal payment pattern arises, which means it is too late to rectify (i.e. the illegal activity has already occurred).

By attaching more detailed information to each transaction or payment instruction (e.g. legal entity information, ultimate beneficial owner), blockchain technology could help reduce the current high false positive rates (currently 99.9%) for suspicious transactions, helping banks to conduct KYC checks at the transaction level (i.e. 'know your transaction'). The distributed ledger would also act as an effective means of recordkeeping for audit purposes, given the data is both irrefutable and immutable. This would allow banks to react more swiftly to regulatory requests, such as furnishing surveillance reports. Duplicative KYC checks for the same clients across different banks should also be reduced if banks can leverage the screening/vetting efforts conducted by other institutions on a shared ledger.

IPR2024-00593
Identitii EX2006

ANTICIPATED COST SAVINGS

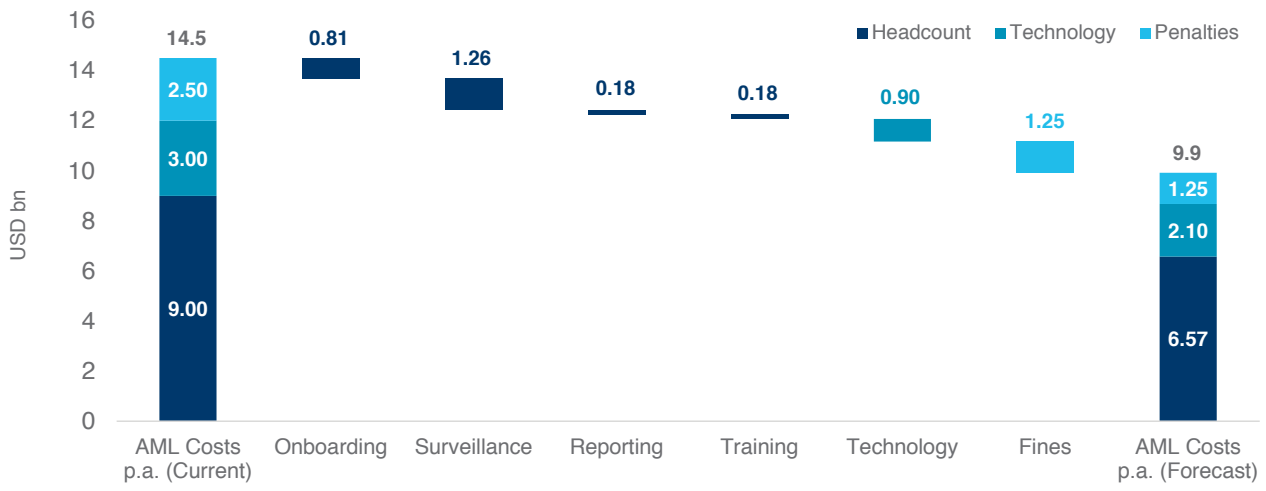
Through the ability of a distributed ledger to enhance both data integrity and accessibility, the manual labour required to conduct KYC checks and review suspected money laundering activity could be significantly reduced. This should help minimise compliance headcount costs. Moreover, blockchain technology also has the capacity to reduce counterparty risk, given the ability to more easily verify client information. With less chance for money laundering activity to slip through the cracks, this can reduce the risks of financial penalties for compliance failings.

We estimate blockchain technology has the capacity to deliver somewhere in the order of USD 4.6 billion in annual AML cost savings to the banking industry (i.e. 32% of current annual costs) in the form of (1) reduced compliance headcount and associated costs (2) lower technology spend and (3) fewer regulatory penalties (see Figure 13).

"THROUGH THE ABILITY OF A DISTRIBUTED LEDGER TO ENHANCE BOTH DATA INTEGRITY AND ACCESSIBILITY, THE MANUAL LABOUR REQUIRED TO CONDUCT KYC CHECKS AND REVIEW SUSPECTED MONEY LAUNDERING ACTIVITY COULD BE SIGNIFICANTLY REDUCED."

IPR2024-00593
Identitii EX2006

FIGURE 13: ANTICIPATED ANNUAL AML COST SAVINGS FROM FINTECH



	AML Costs p.a. (Current)	Annual Blockchain Savings		AML Costs p.a. (Post-Blockchain)
		%	Nominal	
Headcount	USD 9.0bn	27%	USD 2.43bn	USD 6.57bn
Onboarding	USD 4.05bn	20%	USD 0.81bn	USD 3.24bn
Surveillance	USD 3.15bn	40%	USD 1.26bn	USD 1.89bn
Reporting	USD 0.90bn	20%	USD 0.18bn	USD 0.72bn
Training	USD 0.90bn	20%	USD 0.18bn	USD 0.72bn
Technology	USD 3.00bn	30%	USD 0.90bn	USD 2.1bn
Penalties	USD 2.50bn	50%	USD 1.25bn	USD 1.25bn
TOTAL	USD 14.50bn	**32%**	**USD 4.58bn**	USD 9.92bn

Note: USD 9.0 billion in AML headcount costs represent 75% of total estimated 2016 compliance spend of USD 12.0 billion, with technology costs (e.g. surveillance software and KYC software, online training etc.) representing the remaining 25% (i.e. USD 3 billion). AML fines estimated at USD 2.5 billion p.a., based on the average of total fines handed out since 2009

Source: Quinlan & Associates proprietary estimates

IPR2024-00593
Identitii EX2006

ONBOARDING

A 20% annual reduction (i.e. USD 810 million) in headcount costs, given the ability to leverage a shared database of client information to streamline the KYC process and minimise duplicative onboarding efforts for the same client across different banks.

SURVEILLANCE

A 40% annual reduction (i.e. USD 1.28 billion) in headcount costs, driven by the ability of blockchain technology to enrich transaction-level information. This includes the ability to capture and monitor customer data such as legal entity information, which can be supplemented by unique client identifiers. Greater transparency in transaction surveillance could significantly reduce false positive rates and hence the manual checks required by compliance teams to investigate suspicious transactions.

REPORTING

A 20% annual reduction (USD 180 million) in headcount costs, given information is stored – and can be readily accessed – on a distributed ledger, reducing the time needed to both source and validate report data.

TRAINING

A 20% annual reduction (USD 180 million) in costs tied to an overall reduction in AML compliance headcount, reflecting overall headcount savings across compliance personnel in onboarding, surveillance and reporting.

TECHNOLOGY

A 30% annual reduction (USD 900 million) in AML technology spend, reflecting less reliance on both external and proprietary transaction surveillance and monitoring systems.

REGULATORY PENALTIES

A 50% reduction (USD 1.25 billion) in penalties for AML compliance breaches, reflecting higher capture rates of suspicious transaction activity as a result of improved audit and tracing capabilities, as well as richer information being shared via improved messaging infrastructure. Moreover, fines for deficiencies in surveillance software should be substantially reduced with the adoption of blockchain technology.

Overall, we believe meaningful reductions in AML compliance costs, as well as the associated minimisation of reputational risks tied to compliance breaches, should help streamline existing AML compliance processes and encourage the establishment of new payment corridors, reversing the trend of consolidation currently being seen in the correspondent banking space.

IPR2024-00593
Identitii EX2006

INCUMBENT PAYMENT INFRASTRUCTURE DEVELOPMENT

A key industry development in the global payments space was SWIFT's announcement of the launch of its global payment innovation (GPI) initiative in December 2015. The GPI initiative is designed to enhance cross-border transactions whilst utilising SWIFT's messaging platform and global reach. In conjunction with the broader industry, SWIFT has created a new rulebook of service level agreements (SLAs), providing banks with the opportunity to improve collaboration.

With an initial focus on business-to-business payments, the GPI initiative enables corporates to receive enhanced payment services directly from their banks, with features such as same day use of funds, transparent and predictable fees, end-to-end payment tracking and the transfer of rich payment information. Over 70 banks from across the globe have already signed up to the initiative. As SWIFT remains the dominant payment infrastructure globally, we expect quick adoption of new features.

ALTERNATIVE PAYMENT INFRASTRUCTURE SOLUTIONS

Blockchain has widely been touted as the key solution to cutting the time and direct costs of settling ever-increasing volumes of global payments. The most high profile initiatives have been around developing new payment infrastructure using blockchain technology.

Ripple, a US-based provider of blockchain-based banking payments technology, has been one of the leading players in this space. Since 2014, dozens of financial institutions, including HSBC, UBS and Western Union, have announced trials or more advanced commercialisation efforts using Ripple's technology. Most recently, Bank of America Merrill Lynch, Santander, UniCredit, Standard Chartered, Westpac, and Royal Bank of Canada became the founding members of the Global Payments Steering Group (GPSG), which aims to develop rules and governance around the use of Ripple technology for global payments.

IPR2024-00593
Identitii EX2006

Ripple has also developed a crytocurrency called XRP, which can be used as fiat currency for banks to settle their global payments. Typically, the biggest liquidity costs for banks arise from the holding of nostro accounts in different currencies at different banks around the world. With lower costs, we expect to see an exponential increase in low value transactions being processed.

However, the biggest challenge facing correspondent banks in the face of increasing global payment volumes is not one of speed: rather, it is whether individual payments have the required supporting documentation or information to satisfy onerous compliance obligations. This is where many fintech players have focused their efforts (see Figure 14).

FIGURE 14: FINTECH FIRMS AND THE AML VALUE CHAIN

	ONBOARDING				PAYMENT	SURVEILLANCE			REPORTING			
	Customer ID Verification	Sanctions Screening	CDD / Risk Assessment	Risk Rating Applied	Payment Protocol	Transaction Monitoring	Transaction Investigation	Enhanced Review	Periodic Reports	Ad-Hoc Reports	Management Escalation	Regulatory Escalation
SWIFT (Messaging I Financial Crime Compliance)	✓	✓	✓	✓	✓	✓	×	×	✓	✓	×	×
Ripple	×	×	×	×	✓	✓	×	×	✓	✓	×	×
Markit/Genpact-KYC.com	✓	✓	✓	✓	×	×	×	×	✓	✓	×	×
Thompson Reuters-Org ID I Risk	✓	✓	✓	✓	×	✓	×	×	✓	✓	×	×
KYC Exchange	✓	✓	✓	✓	×	×	×	×	×	×	×	×
iSignThis	✓	×	×	×	×	×	×	×	×	×	×	×
Veridu	✓	×	×	×	×	×	×	×	×	×	×	×
Bottomline	×	✓	×	×	×	✓	✓	✓	✓	✓	×	×
Tradle	×	×	×	×	×	×	×	×	✓	✓	×	×
Trulioo	✓	×	×	×	×	×	×	×	×	×	×	×
Identity Mind Global	✓	✓	×	×	×	✓	×	×	✓	✓	×	×
Cambridge Blockchain	✓	×	×	×	×	×	×	×	✓	✓	×	×
Identitii	×	×	×	×	×	✓	✓	✓	✓	✓	×	×
Regulatory DataCorp, Inc.	×	×	✓	×	×	×	×	✓	✓	✓	×	×
Fircosoft	×	✓	×	×	×	✓	×	×	✓	✓	×	×
Dow Jones	×	✓	✓	✓	×	✓	✓	✓	✓	✓	×	×
Bae Systems	×	×	×	×	×	✓	✓	×	✓	✓	×	×
NICE Actimize	×	×	×	×	×	✓	✓	×	✓	✓	×	×
Oracle	×	×	×	×	×	✓	✓	×	✓	✓	×	×

Source: Quinlan & Associates proprietary analysis

IPR2024-00593
Identitii EX2006

AML SOLUTIONS

At the client onboarding stage of the AML value chain, payment infrastructure incumbent SWIFT has developed The KYC Registry to standardise a set of key KYC documentation and data to cover the compliance requirements of different jurisdictions. Banks are able to upload KYC data to a registry which can then be shared with their correspondent banks. By allowing institutions to exchange KYC information safely and securely, The KYC Registry increases transparency while eliminating costly and redundant document exchanges. Other service providers such as Thomson Reuters' Org ID collects data on and verifies a customer's identity. It also provides ongoing monitoring to determine changes in a corporate client's legal entity status.

A number of fintech players are also targeting the surveillance and reporting aspects of the AML value chain, with a view to enhancing KYC checks at the transaction level. Bottomline, for example, offers a range of services including cyber fraud and risk management, financial document automation, financial messaging and payments & cash management services.

Banks use Bottomline for domestic and international payments, effective cash management tools, automated workflows for payment processing and bill review and state of the art fraud detection, behavioral analytics and regulatory compliance. Others firms, such as identitii, offer a universally interoperable information layer that sits above existing and emerging payment infrastructure to provide enriched information about payments. identitii uses tokens to enable banks and customers to attach information & documentation to a payment message, including originator and beneficiary records and attributes.

It is clear there is a huge opportunity to streamline existing AML compliance processes, and fintech firms are jumping at the opportunity. However, in order for any of these blockchain solutions to truly work, they cannot be done on an individual, in-house basis, given the need for a wider consensus mechanism for the technology to be effective. Industry-wide adoption is needed. Only then will the potential cost savings we have outlined in this report materialise.

IPR2024-00593
Identitii EX2006

SECTION 5
CASE STUDY

We had the opportunity to interview the team at identitii, a company that targets the information exchange component of the global payments value chain, which sits on top of the payment settlement infrastructure. Its interoperable protocol can interact with both existing and emergent infrastructure to provide enriched information about payments.

BACKGROUND

In 2015, identitii (formerly called Sparro) worked with select banks during the Accenture Fintech Innovation Lab in Hong Kong to understand the compliance challenges facing banks – namely, the limitation of information that can be transmitted by existing settlement systems to support the timely and less labour-intensive vetting and execution of transactions. Since then, identitii has launched two proof of concepts with top-tier global banks on the use of tokens and blockchain technology to directly target the compliance issues identified. In July 2016, identitii won the SWIFT Innotribe Compliance Challenge, and Innotribe has subsequently engaged with identitii to complete a proof of concept with SWIFT and member banks in Q4 2016 & Q1 2017. Most recently, identitii was recognised as one of KPMG's 2016 Fintech100 Emerging Stars.

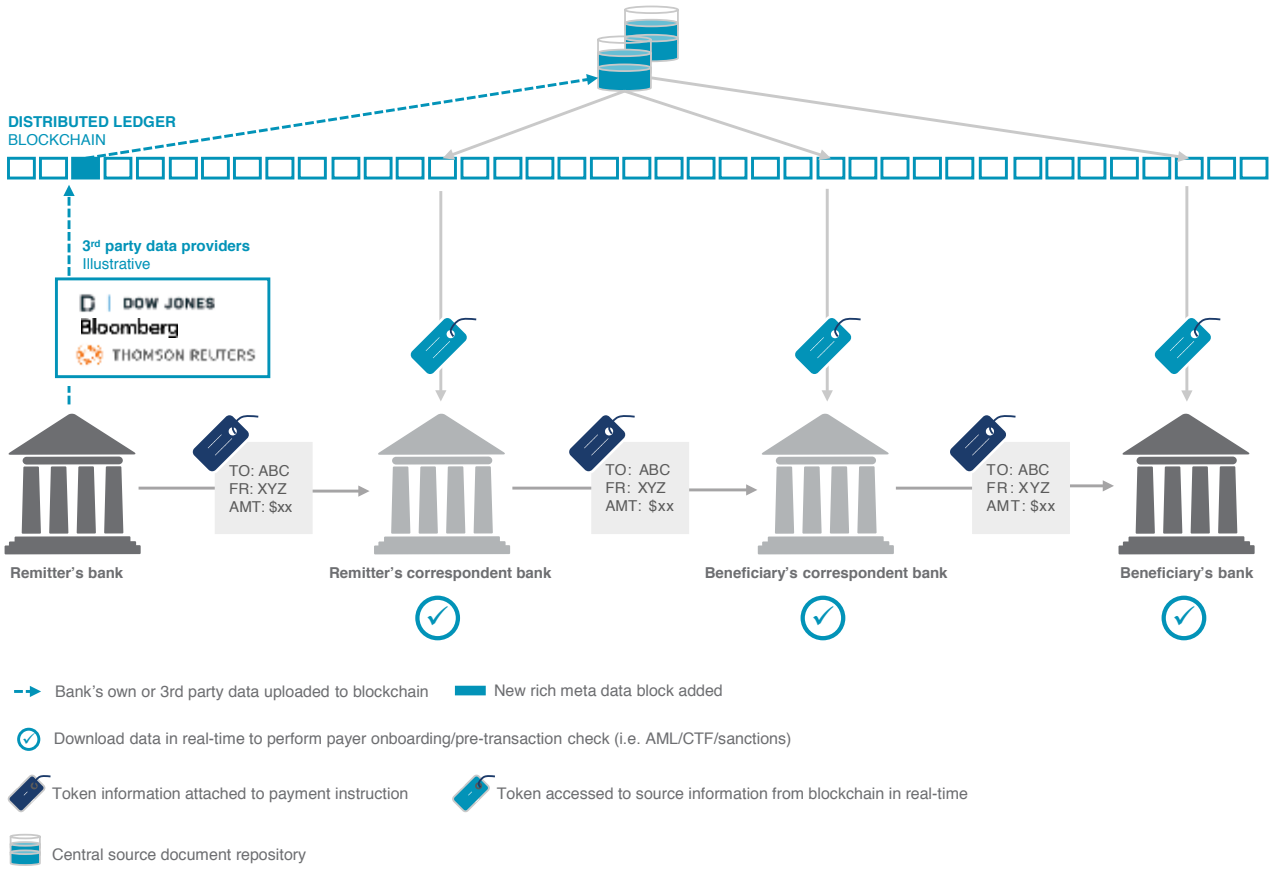
HOW IT WORKS

The company has developed a token which can be attached to a global payment message. The token acts as a portal to rich data (or distributed ledger) and is delivered together with the payment message at each stage of the payment process. At the beginning of a payment process, the remitter's bank is able to upload data including especially detailed information about the remitter from its own sources or via an application programming interface (API) feed from a third party data provider to the distributed ledger, which would represent the 'accounting entry' for the data – the bulk of the source documents would actually be housed in centralised repositories. Examples of the remitter bank's own source documents could include a corporate client's certificate of incorporation or articles of association obtained as part of the client onboarding process.

Banks further along the payment process, by accessing the token attached to the payment message, would then have access to remitter and/or beneficiary data (see Figure 15).

IPR2024-00593
Identitii EX2006

FIGURE 15: IDENTITII TOKENS



Source: Quinlan & Associates analysis

IPR2024-00593
Identitii EX2006

REAL-TIME KYC

The protocol envisaged would have the ability for feeds from third party data providers to be accessed as changes occurred, so that the correspondent/ beneficiary bank is also able to gain access to the most up-to-date data, such as changes to a remitting company's ultimate beneficial owner or even data about a fellow bank further down the payment chain.

STRAIGHT THROUGH PROCESSING

In the fully integrated version of identitii's technology, integration with a bank's systems would mean that downloaded data can be fed directly into a bank's compliance engines, including KYC/customer due diligence, fraud monitoring, sanctions screening and AML systems. Such solutions are very compelling for the banks as they offer straight through processing, doing away with much of the manual collection and review of documentation that is currently required at each stage along the global payment transaction process to satisfy compliance obligations.

The reduced time and cost that straight through processing offers can reduce the operating costs of banks, and provide peace of mind as knowing the nature of the transaction will allow banks to maintain and re-establish their correspondent bank relationships, opening up more revenue opportunities.

END USER BENEFITS

Access to a rich dataset opens up the payment system to further commercial advantages for end-users (i.e. customers, for example, can experience real-time tracking of payments and easier matching of invoices to payments).

FUTURE AGENCY MODEL?

As richer information is built up in robust and centralised repositories and as KYC/CTF regulation becomes more sophisticated, we believe that we may move to the point where any KYC, sanctions & CTF checks performed by other parties along a global payment process would be accepted bona fide by the legal and regulatory requirements in different jurisdictions where the banks are domiciled or operating, thereby reducing the duplicative compliance processes that are commonplace today.

Currently, over 11,000 financial institutions use SWIFT, one of the most popular payment messaging systems for international payments. identitii has focused on ways to enhance the relatively stable and robust nature of such existing financial markets infrastructure. The payload of the rich data remains on the distributed ledger and centralised repositories such that the legacy infrastructure is not overloaded. We believe that by overlaying a richer data layer onto proven systems like SWIFT through their token technology, this will allow for much greater adoption and likelihood of becoming a global standard. At the same time, the intra-operability of their technology means that it can also be used in conjunction with emergent cross-border payments systems being developed by players such as Ripple.

IPR2024-00593
Identitii EX2006

SECTION 6
HOW CAN WE HELP?

Our consultants have worked with a number of international banks in terms of evaluating their AML compliance programs and potential engagement with fintech providers. The scope of our project work typically includes:

COMPLIANCE

Perform a comprehensive review and analysis of the bank's AML value chain, focusing on pressure points in current operations, e.g.:

- Review of current onboarding, surveillance and reporting processes to optimise existing procedures
- Review of cost drivers across technology, personnel and other expenses

FINTECH

Develop a detailed strategic plan for the bank's fintech efforts, supported by clear financial and operational targets, together with development milestones, e.g.:

- Assess the impact of fintech on existing cost and revenue streams
- Appraise the size and direction of opportunities for implementing fintech across the bank from both an internal process and client perspective
- Determine the most appropriate fintech collaboration model and governance framework, including product validation and investment considerations

 © COPYRIGHT QUINLAN & ASSOCIATES

IPR2024-00593
Identitii EX2006

QUINLAN
&ASSOCIATES

STRATEGY WITH A DIFFERENCE

Copyright © 2016 Quinlan & Associates.

All rights reserved. This report may not be distributed, in whole or in part, without the express written consent of Quinlan & Associates. Quinlan & Associates accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Quinlan & Associates. This report is not financial or investment advice and should not be relied upon for such advice or as a substitute for professional accounting, tax, legal or financial advice. Quinlan & Associates has made every effort to use reliable, up-to-date and comprehensive information and analysis in this report, but all information is provided without warranty of any kind, express or implied. Quinlan & Associates disclaims any responsibility to update the information or conclusions in this report. Quinlan & Associates accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. Quinlan & Associates engages in and seeks to do business with some of the companies mentioned in its reports.

ABOUT US

Quinlan & Associates is an independent strategy consulting firm specialising in the financial services industry.

We are the first firm to offer end-to-end strategy consulting services. From strategy formulation to execution, to ongoing reporting and communications, we translate cutting-edge advice into commercially executable solutions.

With our team of top-tier financial services and strategy consulting professionals and our global network of alliance partners, we give you the most up-to-date industry insights from around the world, putting you an essential step ahead of your competitors.

Quinlan & Associates. Strategy with a Difference.

CONTACT US

@ info@quinlanandassociates.com | www.quinlanandassociates.com | (+852) 2618 5000

Level 19, Two International Finance Centre, 8 Finance Street, Central, Hong Kong SAR

IPR2024-00593
Identitii EX2006