Correspondent Banking as a Vector of Illicit Financial Flows

A CASE STUDY OF BGFIBANK DRC



ANTI CORRUPTION DATA COLLECTIVE

PPLAAF

Correspondent Banking: A Vector of Illicit Financial Flows
November 2026

This research is part of the Governance & Integrity Anti-Corruption Evidence (GI-ACE) programme which is hosted by the Centre for the Study of Corruption, University of Sussex and funded by the UK government's Foreign, Commonwealth & Development Office (FCDO) through its Global Research and Technology Development portfolio. GI-ACE generates actionable evidence that policymakers, practitioners and advocates can use to design and implement more effective anti-corruption initiatives. The views expressed here do not necessarily reflect the UK Government's official policies.

About the Anti-Corruption Data Collective (ACDC)

The Anti-Corruption Data Collective (ACDC) is a non-profit group of leading investigative journalists, academics, policy experts and data scientists that leverages public and private data to expose transnational corruption, illicit financial activity and corporate opacity. Our research and investigations seek to document and reduce the harms that corruption causes to human security, democratic participation and environmental sustainability: to People, Politics and Planet.

About the Platform to Protect Whistleblowers in Africa (PPLAAF)

The Platform to Protect Whistleblowers in Africa (PPLAAF) is a non-governmental organisation established in 2017 to protect whistleblowers, investigate their disclosures, advocate on their behalf, and undertake strategic legal actions when their revelations concern matters of public interest for African citizens.

Every effort has been made to verify the accuracy of the information contained in this report.

All information was believed to be correct as of November 2026. Nevertheless, ACDC and PPLAAF do not accept responsibility for the consequences of its use for other purposes or in other contexts.

Table of Contents

EXECUTIVE SUMMARY 04

PART 1: RELATIONSHIPS AND RISKS IN CORRESPONDENT BANKING 08

1.1. What Is Correspondent Banking? 08

1.2. Correspondent Banking KYC 09

1.3. Ongoing AML/CFT Responsibilities 09

1.4. De-risking & Risk-Based Approaches 09

PART 2: LEGAL LIABILITY OF CORRESPONDENT BANKS 11

2.1. Sanctions 12

2.2. Public Leaks 12

PART 3: CASE STUDY: CONGO HOLD-UP AND BGFIBANK 14

3.1. Data Sources 14

3.2. BGFIBank DRC and the Congo Hold-Up 14

3.3. Systemic Breakdown 16

PART 4: SYSTEMIC FAILURES 23

4.1. Easy Obfuscation and Failure to Challenge 23

4.2. Invoices as Proof 30

4.3. De-Risking and Suspicious Transactions 32

PART 5: RECOMMENDATIONS 34

5.1. To Regulators and Law Enforcement Authorities 34

5.2. To Correspondent Banks 35

5.3. To Civil Society and Media 36

5.4. To Authorities in Respondent Countries, Including the DRC 36

CONCLUSION 37

ANNEXES 38

ENDNOTES 42

Executive Summary

An estimated $0.8-2 trillion[1] is laundered globally each year. Despite technological innovations in the global financial system, including the proliferation of stateless digital asset transactions recorded on the blockchain, transfers of funds, both licit and illicit, between countries and currencies still rely on a much older system: correspondent banking.

In correspondent banking, a third-party bank uses its access to a specific jurisdiction or currency to process transactions on behalf of other financial institutions. This system underpins most of the volume of global cross-border payments, which reached an estimated $195 trillion in 2024.[2]

The banks providing these correspondent banking services have no contractual connection to either the individual sender or recipient of the funds. Instead, they provide services to smaller 'respondent' banks around the world, often earning relatively low transaction fees for their services. In doing so, they expose themselves to the risk of processing illicit transactions that have been accepted by the respondent bank. This dynamic has led banks to 'de-risk,' ending their relationship with the respondent bank entirely, potentially leaving customers, or even entire countries, cut off from the global financial system. Those that remain may have a higher risk appetite or spend less on compliance than their competitors, leaving cross-border transactions dangerously under scrutinised for signs of money laundering or financing of terrorism.

REGULATION AND AML RESPONSIBILITY

In a necessarily international domain, responsibility for ensuring that correspondent banks comply with obligations to prevent money laundering and the financing of terrorism (ML/FT) rests with national regulators. Recommendations from the Financial Action Task Force (FATF) provide guidance for financial institutions and national regulatory and supervisory authorities and are transposed into binding national legislation. However, when things go wrong, enforcement against banks for AML/CFT breaches in their correspondent banking relationships often arises from economic sanctions programmes, where there is a clear geopolitical incentive for authorities, typically from the United States (US), to hold banks accountable. This enforcement has mainly targeted foreign respondent banks, leaving their US correspondent banks untouched. Meaningful accountability for correspondent banks facilitating the laundering of the proceeds of corruption and kleptocracy is far rarer, often relying on public outcry after reporting based on leaked data.

THE CASE OF BGFIBANK DRC

This paper draws on analysis of leaked data to examine a case in which correspondent banks processed millions of dollars in suspicious transactions for a private bank that had been captured by the ruling elite of the Democratic Republic of Congo, BGFIBank DRC.

The case of BGFIBank DRC exemplifies how a respondent bank can be instrumentalised by a kleptocratic regime to facilitate the movement of illicit financial flows around the world through correspondent banks. Run by, and partly owned by, close relatives of then-president Joseph Kabila (in office, 2001 – 2019), BGFIBank DRC was revealed in the 2021 Congo Hold-Up investigations by a consortium of media and civil society organisations to have facilitated the wholesale looting of the DRC's state assets and natural resources to benefit Kabila and his inner circle.

Despite having been contacted repeatedly by Congo Hold-Up consortium partners, the BGFIBank Group had declined to respond.[3] That is until it issued a statement on 24 November 2021 in which it questioned the authenticity of the leaked documents, said it disapproved of any questionable practices that may have occurred in the past at its Congolese subsidiary and said it had taken corrective measures from 2018.[4] Joseph Kabila did not wish to answer the questions put to him by Congo Hold-Up consortium partners.[5] His lawyers later rejected the findings.

Multiple international correspondent banks worked with BGFIBank DRC to send money out of the DRC for many years. Major international banks including Citibank and Commerzbank, as well as FIMBank in Malta and BMCE Bank in Madrid, processed transactions for BGFIBank DRC that displayed glaring red flags for financial crime. When asked about these transactions in 2021, Citibank and Commerzbank did not comment on them specifically but did emphasise their general due diligence and compliance procedures. FIMBank declined to answer, citing client confidentiality, and BMCE Bank (now Bank of Africa Europe) said that its policies for preventing financial crime were "fully in line with the most demanding international standards".[6] Moreover, when the risks became too high for some of these institutions, the main correspondent bank that remained was a sister financial institution, BGFIBank International, based in Paris, that allowed thousands of suspicious transactions to pass through its accounts. Due diligence was minimal or performative: too few questions were asked and the documents provided in response were rarely checked.

Taking advantage of a unique dataset to analyse these transactions in detail, this paper finds that amid kleptocratic capture of key domestic institutions, natural resource wealth and inbound investment, BGFIBank DRC processed some $1.6 billion in outgoing foreign transfers from the DRC between 2011 and 2020, the period covered by the data leak. The following banks were responsible for processing the bulk of this volume, including a significant share with the hallmarks of illicit financial flows linked to corruption, kleptocracy and state capture.

- Commerzbank processed 76% of BGFIBank DRC's foreign transfers appearing in the leaked data between 2011 and 2016, equivalent to 68% of the transferred dollar value: almost $800 million. The bank appears to have waved through a $1 million payment to Congo Construction Company (CCC), a shell company used to channel bribes to Kabila's circle, from Société de Gestion de Péage au Congo (SOPECO), a firm owned by an associate of CCC's directors that was under investigation in DRC for embezzlement.

- Malta's FIMBank processed international transactions worth more than $250 million during the nine-year period covered by the leak, 83% of which was transferred before 2016. FIMBank ignored explicit warnings from peer financial institutions about Glory Group, the successor to Congo Futur, which had been sanctioned by the US for financing Hezbollah. FIMBank allowed Glory Group companies to funnel nearly $140 million abroad, including transactions justified with invoices for different amounts.

- In the summer of 2016, Citibank approved at least $17 million in transfers from Sicomines, a Chinese-Congolese joint venture, to the BGFIBank DRC accounts of CCC. Large transfers were justified with strikingly vague descriptions, including "contract costs" and "payment". BMCE Bank, the Madrid-based subsidiary of Morocco's BMCE Bank of Africa (now Bank of Africa), used Citibank to clear large, dollar denominated payments for BGFIBank DRC, including a $9 million payment from Sicomines to CCC.

- From 2016 onwards, after Commerzbank cut ties with BGFIBank DRC, BGFIBank International in Paris executed approximately 71% of all outgoing transactions from its Congolese subsidiary. PPLAAF estimates that $450 million in suspicious funds were moved out of BGFIBank DRC and into the international financial system by BGFIBank International, including over $30 million to and from entities connected to the presidential administration.

> Over 40% of its transactions are potentially suspicious. Although compliance officers at BGFIBank International repeatedly raised concerns, these were routinely overridden or answered with back-dated documents and false paper trails produced by BGFIBank DRC executives in Kinshasa. The BGFIBank Group, BGFIBank International's parent company, had declined to respond to the Congo Hold-Up consortium before publication.[7]

Because the kind of micro-level data on transactions available from the Congo Hold-Up leak is mostly shielded from public view, correspondent banks have been overlooked as an enabler of dirty money. Yet, the problems highlighted by BGFIBank DRC are current and global. A New York Times investigation published in October 2026 showed how Zhejiang Chouzhou Commercial Bank, a regional Chinese lender providing US dollar access to nearly 70 other banks, many of them in high-risk jurisdictions, gave Russian front companies indirect access to accounts at major US banks.[8] Zhejiang Chouzhou did not respond to the newspaper's detailed questions, and an executive of its correspondent-banking division declined to comment when approached in person.[9]

Legal accountability mechanisms do exist for correspondent banks. In an unprecedented move, France's National Financial Prosecutor (Parquet National Financier, or PNF) opened a preliminary investigation into BGFIBank International (now BGFIBank Europe) for "aggravated money laundering" in 2022, after the publication of the Congo Hold-Up investigations. When the investigation was announced in June 2022, BGFIBank International did not respond to AFP's requests for comment, and BGFI Gabon declined to comment, saying that the matter concerned a subsidiary.[10] Yet, if the goal is to prevent all kinds of illicit financial flows, the current system is clearly not working.

Much can be achieved simply by improving the way the existing framework is applied. For example, national supervisors should look more closely at correspondent banking relationships with high-risk jurisdictions and at de-risking decisions, while correspondent banks should properly scrutinise the responses they receive once a transaction is flagged. The commencement of direct supervision by the EU Anti-Money Laundering Authority (AMLA) in 2028 and recent advances in technology provide a further opportunity for this essential financial service to be more effective, both in cost and in practice, while deterrent fines and criminal prosecutions, where applicable, would raise the cost of non-compliance for correspondent banks which continue to flout the rules.

RECOMMENDATIONS

Law enforcement, regulators, supervisors and banks themselves on both sides of correspondent banking relationships should implement measures that ensure:

- Enhanced monitoring and scrutiny of correspondent banking relationships with the highest risk of facilitating illicit financial flows, especially with banks exhibiting signs of political capture. Suspicious transactions should be frozen until proven legitimate, with clear documentation of investigations. The independence of auditors should be verified.

- Information sharing and coordination between banks, regulatory and supervisory authorities, and law enforcement, including around de-risking decisions, suspicious transactions, scope for compliance improvements, and high-risk structures and patterns in correspondent banking relationships.

- Responsible use of artificial intelligence in AML compliance and suspicious transaction reporting, ensuring that any efficiency gains translate into better-quality human review of alerts rather than reductions in compliance staff.

- Safe and effective whistleblower channels and protections, explicitly covering compliance officers and staff of respondent banks and requirements to act upon whistleblower reports.

- Accountability for processing illicit financial flows, including deterrent and proportional fines, and criminal liability for individuals involved in breaching AML / CFT laws, where appropriate.

Part 1:
Relationships and Risks in Correspondent Banking

1.1. WHAT IS CORRESPONDENT BANKING?

Correspondent banking refers to bilateral relationships between banks which allow them to provide cross-border payment services for their customers through accounts held at another bank. With another financial institution acting as an intermediary, financial institutions can carry out business and offer services they could not otherwise provide due to the lack of a presence in another jurisdiction. Originating in medieval Europe to allow merchants to handle local payments, correspondent banking has undergone changes and modifications as cross-border payment technology has changed from paper ledgers to the telegraph, to early electronic payment systems and today's digital era. Correspondent banking continues to have an essential role in global trade and economic activities, remaining a key component of the global financial services industry.

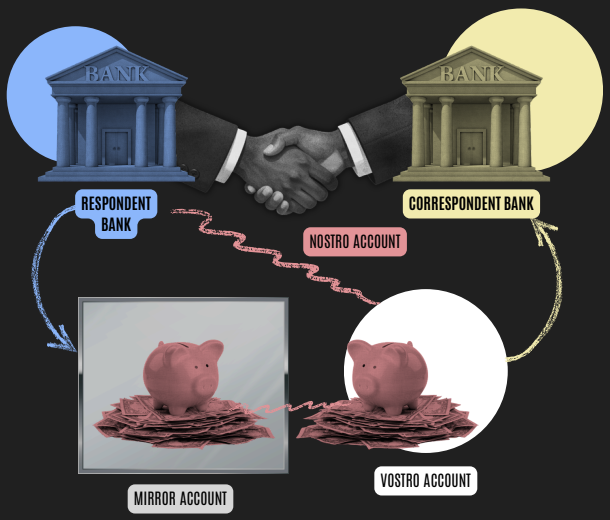
The services provided by the correspondent bank can take different forms. The three main ones are as follows:[11]

- Traditional correspondent banking, in which the correspondent bank executes payments on behalf of the respondent and its customers, without granting the respondent bank's customers access to the correspondent account.
- Nested correspondent banking, in which a number of respondent banks, which are sometimes part of a corporate group or network, access a single correspondent bank via a respondent bank which holds the direct relationships with the correspondent.
- Payable-through accounts, in which the direct respondent bank allows its customers to access the account it holds at a correspondent bank themselves.

Nostro/Vostro accounts

A "nostro account" ('ours' in Italian) is an account in a foreign currency held by a respondent bank on the books of a correspondent bank which acts as the service provider. A "vostro account" ('yours' in Italian) is an account in domestic currency held by a correspondent bank on behalf of the respondent bank.[12]

In the correspondent banking system, this distinction is a question of perspective. The nostro account is the account of the bank receiving the correspondent banking services (i.e. the respondent bank), while the vostro account is the account held by the bank providing those services (i.e. the correspondent bank).[13] In some cases, the respondent bank can have a mirror nostro account, so that it can keep track of the money transfers in its books.



Although best explained in simple and bilateral terms, in reality correspondent banking is a complex system made up of tens of thousands of active cross-border relationships around the world.[14] This complexity has resulted in a relatively opaque system which has the potential for misuse by those seeking to commit fraud, money laundering, or terrorism financing.

1.2. CORRESPONDENT BANKING KYC

Before entering a correspondent relationship with a respondent bank, a correspondent bank is generally required to assess the credibility and compliance with legal and regulatory frameworks of its respondent bank. The correspondent bank is required to undertake a review of the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) controls of the respondent bank, including its own Know Your Customer (KYC) procedures. The respondent bank has to provide this information, and the correspondent bank has, to some extent, to trust that the respondent bank, who holds the contractual relationship with the payer and recipient, is being forthcoming with the information it shares.

1.3. ONGOING AML/CFT RESPONSIBILITIES

In order to avoid breaching AML/CFT regulations due to exposure to illicit financial flows through the respondent bank, correspondent banks are under an obligation to conduct regular due diligence checks throughout the correspondent relationship.

Correspondent banks must monitor the overall relationship and watch for unusual activity, including deviations from normal transaction patterns. This includes ensuring that transaction data and accompanying documentation (such as invoices) are complete and transparent. Correspondent banks must also screen senders and recipients against sanctions lists, and work to identify suspicious patterns such as circular fund flows, pass-through transactions designed to obscure origins, or rapid movement of large sums without clear commercial purpose. If any aspects of a transaction are flagged by a correspondent bank's monitoring system, they should request additional information from the respondent bank and, if the response is unsatisfactory or incomplete, reject the transaction, consider filing a suspicious transaction report and reassess the relationship. As payments move from one bank to another, the process can become slower, more opaque, and more challenging to track, ultimately driving up complexity and cost.

To prevent money laundering, terrorist financing, and other types of fraud or illicit activities, correspondent banks must continuously perform thorough customer due diligence on their respondent bank commensurate with the degree of risk identified. If one of the regular due diligence assessments of the respondent bank leads to the identification of an illicit activity, a risk becomes unmanageable or the respondent bank fails to comply with one of its obligations, national-level AML/CFT obligations will likely require the correspondent bank to end the correspondent banking relationship and, if necessary, alert the relevant authorities.

1.4. DE-RISKING & RISK-BASED APPROACHES

Even while cross-border transactions have grown, there has been a universal and gradual thinning and concentration of the correspondent banking network since 2008. Particularly in the early 2010s, fear of regulatory and judicial sanctions and reputational damage drove many financial institutions around the world to drastically reduce their correspondent banking relationships, cutting ties with banks operating in what were considered to be high-risk jurisdictions (i.e. jurisdictions where governance and supervision over illicit financing were considered weak).

This trend emerged in response to a strengthening of AML / CFT standards for the industry but had unintended consequences. International organisations, such as the World Bank and the Financial Action Task Force (FATF) criticised de-risking for concentrating correspondent banking relations between a small number of institutions, usually excluding low-income countries and emerging markets from access to global capital. It also created new challenges by forcing banks in high-risk jurisdictions to find alternative ways of maintaining their access to the cross-border payment system, lengthening the "payment chain" by asking other banks maintaining correspondent relations to act as intermediary for them.[15] Worse still, it even led to the increased use of informal channels by the excluded banks to maintain access to the cross-border system, as noted by the FATF.[16]

Longer chains can concentrate risk in a few niche intermediaries. According to correspondent banking compliance data cited by The New York Times in 2026, Zhejiang Chouzhou Commercial Bank provides dollar accounts to nearly 70 other banks, most of which otherwise lack direct access to the US financial system; by comparison, ICBC, the world's largest bank by assets, provides dollar access to 20 banks and HSBC Bank in London to seven.[17]

To stop banks pulling out of correspondent relationships entirely, the FATF recommendations updated in 2016 require that states establish a risk-based approach as one of the cornerstones of their AML/CFT framework. Based on informed analysis, states are only required to adopt measures proportionate to the specific money laundering and terrorism financing risks in their jurisdictions.[18] Consequently, the risk-based approach encompasses a risk management strategy specifically tailored to each individual case analysis. However, the downside is that applying this approach entails increased compliance costs, higher fines and reputational risks.[19] By promoting a case-by-case analysis, it also works against harmonisation within the correspondent banking system.

As well as the FATF recommendations for national regulators (see Annex A), standards promoted by international organisations targeting supervisory authorities, such as the Basel Committee on Banking Supervision,[20] and banks themselves such as the Wolfsberg Group,[21] provide guidance to help banks manage the risks of correspondent banking relationships. In the European Union, the Anti-Money Laundering Directives require enhanced due diligence for cross-border correspondent relationships with respondent institutions from third countries, an obligation carried into the directly applicable Anti-Money Laundering Regulation (EU) 2024/1624, which applies from July 2027. In the United States, Section 312 of the USA PATRIOT Act requires enhanced due diligence on correspondent accounts held for certain foreign banks, and Section 313 prohibits correspondent accounts for foreign shell banks.

However, in a joint fact sheet issued in August 2016, the US Treasury and federal banking agencies clarified that there is no general requirement for US banks to conduct due diligence on the customers of their foreign respondent banks (sometimes called 'know your customer's customer'). The correspondent is expected instead to assess whether the respondent is itself capable of monitoring its own clients.[22] This is broadly consistent with the recommendations from FATF, BCBS and Wolfsberg, which emphasise understanding and managing the risks emerging from the geographies, client profiles, downstream banking relationships, ownership and political entanglements of the respondent bank. Banks are meant to establish clear responsibilities and obligations commensurate with the level of risk. This can include real-time transaction monitoring for particularly high-risk institutions.

However, despite the promotion of a risk-based approach, large international banks have continued to terminate correspondent banking relationships and the number of active correspondents in each region continues to fall,[23] further impacting global financial stability.

For respondent banks, obligations are typically set out in the national AML/CFT legislation. The limits of the framework therefore lie less in the absence of rules than in the way they are applied and supervised, as the case study in Section 3 demonstrates.

Part 2:
Legal liability of correspondent banks

There has been some enforcement against banks providing correspondent banking services and the fines levied are often significant. Financial regulators have extensive powers, the ability to issue punitive fines, and, in the right circumstances, the liability can even reach a criminal threshold. However, such accountability is largely restricted to specific circumstances.

2.1. SANCTIONS

Fines for banks that provide correspondent banking services in violation of United States sanctions are the most significant. This often involves violations of the International Emergency Economic Powers Act (IEEPA)[24] which grants sanction authority to the US President and the Trading with the Enemy Act (TWEA),[25] which restricts transactions with an 'ally of the enemy' of the United States at a time of war.

- In 2014, the French bank BNP Paribas agreed to a fine and forfeiture of $8.9 billion after pleading guilty to conspiring to violate both IEEPA and TWEA by "providing dollar clearing services to individuals and entities associated with Sudan, Iran, and Cuba – in clear violation of US law" and "continued to engage in this criminal conduct even after being told by its own lawyers that what it was doing was illegal". From 2004 to 2012, BNP Paribas moved $8.8 billion through the US financial system in violation of US economic sanctions.[26]

- In 2019, the British bank, Standard Chartered Bank, admitted to processing financial transactions through US financial institutions for the benefit of sanctioned Iranian entities over a period from 2007 to 2011, and agreed to a fine and forfeiture of over $1 billion across multiple US and UK authorities (the UK transactions covered the period 2010 to 2013). Both countries specifically refer to the Dubai, UAE branch of Standard Chartered which allowed Iranian-linked accounts to be opened.[27]

- In 2012, the British Bank HSBC agreed to a forfeiture of $1.256 billion for partly "failing to conduct appropriate due diligence on its foreign correspondent account holders. The HSBC Group violated IEEPA and TWEA by illegally conducting transactions on behalf of customers in Cuba, Iran, Libya, Sudan and Burma" - all sanctioned countries. There was also an anti-money laundering violation (the Bank Secrecy Act in the United States)[28] related specifically to their processing of funds for Mexican drug cartels.[29]

- In 2015, the German Bank Commerzbank agreed to pay a fine and forfeiture of $1.45 billion to law enforcement and financial regulators in the United States for "willfully failing to have an effective anti-money laundering (AML) program, willfully failing to conduct due diligence on its foreign correspondent accounts, and willfully failing to file suspicious activity reports" in relation to transactions on behalf of Iranian, Sudanese, Cuban and Burmese entities.[30]

The United States is aggressive in investigating and prosecuting firms that fail to prevent misuse of the US financial system, especially where it is relevant to US foreign policy interests. In sanctions cases, enforcement has focused on foreign institutions, while US correspondents unwittingly involved are rarely penalised. As recently as September 2026, the US government imposed restrictions on two foreign banks that had used the correspondent system to help Iran access the dollar on behalf of the Islamic Revolutionary Guard Corps. By contrast, although US banks can be held liable for processing prohibited transactions even when acting only as correspondents, the Treasury has discretion over which cases it pursues. A former senior Treasury official told The New York Times that it would be difficult to imagine a US bank being penalised for unwittingly playing a role in a sophisticated sanctions-evasion scheme.[31]

The supremacy of the US dollar in global financial transactions also acts as an incentive for countries to protect the integrity of their financial system. Financial institutions cannot risk losing the ability to process dollar transactions and therefore effective enforcement prevents those deemed to be 'an ally of the enemy' from accessing global financial markets – a clear positive for the foreign policy interests of the United States.

While aggressive and effective enforcement is positive, it cannot be left to one country to police the global financial system. This is especially problematic where it is clear the most extensive enforcement is in relation to foreign policy goals. It is essential that financial regulators in other parts of the world also enforce against these regulatory violations and criminal behaviour. As the super-regulator of the second most used currency globally, the newly created EU Anti-Money Laundering Authority (AMLA), can take a key role in this as they commence direct supervision in 2028.[32]

2.2. PUBLIC LEAKS

In 2022, the Danish bank Danske Bank agreed to a $2 billion criminal forfeiture[33] following an investigation into their Estonian branch operating as a 'laundromat' for illicit financial flows from Russia and Azerbaijan.[34] The scandal came to light through internal whistleblowing by Howard Wilkinson and subsequent reporting by the Danish newspaper Berlingske.[35] They were able to show the scale of shell company creation by the bank and billions of dollars they processed for their customers.

In this case again, it was the respondent bank which was held to account under extraterritorial jurisdiction of the United States for defrauding the US banks that provided it with correspondent banking services.

Wilkinson, who served as head of Danske Bank's trading unit in the Baltic region until 2014 stated in testimony to a Danish parliamentary hearing: "No one really knows where this money went. All we know is that the last people to see it were these three large banks in the US. They were the last check and, when that failed, the money was into the global financial system".[36]

The three banks, Deutsche Bank, JP Morgan and Bank of America, were approached by US criminal investigators in the same month as Howard Wilkinson's testimony.[37] It is difficult to establish criminal liability for correspondent banks as they have no obligation to undertake individual CDD on the respondent bank's customers. When asked by journalists in 2019 about an investigation by the US Federal Reserve into their risk management and control systems as a result of their ties to Danske Bank in Estonia, Deutsche Bank stated that the "only relationship (as a correspondent bank) is with the bank and the bank itself has the responsibility to check its own client (and) to monitor the transaction"[38] They were later fined $186 million by the US Federal Reserve in 2023 for their slow progress in making changes to their AML controls.[39] To our knowledge, no penalties have been imposed on JPMorgan or Bank of America in connection with Danske Estonia.

It should be noted that the Nordic bank Nordea, the second largest bank in Denmark, agreed in August 2024 to pay the New York Department of Financial Services $35 million in administrative penalties for their involvement in the same scheme as Danske. They were partially fined for "failure to conduct proper due diligence of its correspondent bank partners".[40] In June 2026, Danish prosecutors sought a record criminal fine of DKK 6.6 billion (about €880 million) against Nordea for AML failings between 2012 and 2015, which the bank contests. On 9 November 2026, Nordea were acquitted on five of the seven counts and were fined DKK 155 million (about €20 million).[41]

Three of the European correspondent banks whose failures are documented in this paper — FIMBank (Malta), Commerzbank (Germany), and BMCE Bank (Spain) faced no meaningful enforcement action from their home-country supervisors specifically in connection with their correspondent banking relationships with BGFIBank DRC.

The Bank of Spain's 2019 sanction against BMCE Bank cited governance failures but made no reference to BGFIBank DRC or Afriland First Bank, another Congolese bank. The Maltese Financial Services Authority did sanction FIMBank in 2020 but there was no mention of its processing of Glory Group/Hezbollah-linked transactions (see case-study in Section 3 below).[42] BaFin issued no specific findings on Commerzbank's BGFIBank DRC exposure, despite Commerzbank having paid $1.45 billion in the United States in 2015 for separate sanctions and AML failures.

This asymmetry is not coincidental: it reflects a structural gap in supervision that the creation of AMLA is designed, in part, to address. Until then, this gap will continue to be exploited by illicit actors who understand that European correspondent banks face a fraction of the enforcement risk of their American counterparts. It was revealed in June 2022 that the French Parquet National Financier had commenced a preliminary investigation into the Paris-headquartered BGFIBank International for "aggravated money laundering".[43] However, there is little news on whether this has progressed further despite the large amount of evidence made public in the Congo Hold-Up investigations.

Investigative journalists and civil society can try to push for accountability against financial institutions that fail to meet their legal and regulatory obligations. However, they are limited to what is contained in the evidence. Access to internal emails makes it easier to demonstrate what correspondent banks knew in relation to BGFIBank DRC.

It is incumbent on law enforcement and regulators to use their powers to not only aggressively investigate the respondent banks who clearly facilitate money laundering, but also the wilful blindness of correspondent banks who maintain weak risk management and control systems and benefit from the same transactions.

Part 3:
Case Study: Congo Hold-Up and BGFIBank

The case of BGFIBank DRC offers a uniquely detailed empirical window into how each of the obligations set out above was tested in practice and systematically failed. Unlike theoretical analyses, the Congo Hold-Up leak provides direct access to the internal communications of the respondent bank and its correspondent banks, revealing not only what went wrong, but precisely what was communicated, what was requested, and what was ultimately ignored.

3.1. DATA SOURCES

This paper draws on the Congo Hold-Up leak, comprising over 3.5 million internal documents from BGFIBank, including bank statements, contracts, correspondence, and internal emails. The dataset covers the period 2010 to 2020.

This section offers a rare view into how correspondent banks repeatedly failed to meet their obligations to scrutinise high-risk transactions and reject payments lacking a clear commercial purpose. Drawing on the Congo Hold-Up leak, it shows how foreign banks processed hundreds of millions of dollars in suspicious transfers over nearly a decade, including payments linked to sanctioned networks, shell companies, politically exposed persons, and alleged embezzlement schemes. Through case studies of four correspondent banks - FIMBank (Malta), Citibank (USA), BMCE Bank (Spain), and BGFIBank International (France/Paris) - the section examines how these relationships worked in practice and how anti-money laundering controls broke down.

3.2. BGFIBANK DRC AND THE CONGO HOLD-UP

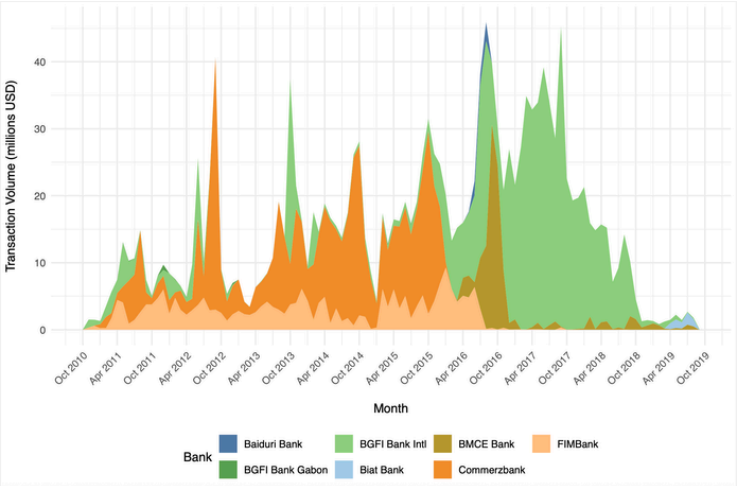
In November 2021, the Platform to Protect Whistleblowers in Africa (PPLAAF) and Mediapart made public that they had obtained a large leak from BGFIBank, a bank whose Congolese subsidiary was closely tied to the regime of former President Joseph Kabila. In what became known as the Congo Hold-Up, PPLAAF was provided with over 3.5 million internal bank documents, including contracts, bills, corporate records, bank statements, and correspondence. The leak provided unprecedented insights into the workings of a bank captured by the Kabila regime. Based on these documents, journalists and non-governmental organisations were able to uncover and report on staggering levels of corruption and theft from the Congolese people, documented in over 100 articles published as part of Congo Hold-Up.

BGFIBank DRC was founded in 2010 as a subsidiary of BGFIBank, headquartered in Gabon. As a private institution, the bank was majority owned by its parent company BGFIBank Gabon, yet friends and family of Joseph Kabila, President of the Democratic Republic of Congo at the time, were heavily involved in running the bank, including his adoptive brother Francis Selemani, who served as the subsidiary's CEO from 2012 to 2018. Moreover, Kabila's sister Gloria Mteyu owned 40% of the subsidiary in DRC. Over the next ten years, the BGFIBank DRC became the 7th largest bank in the country, processing transactions worth millions on a daily basis.

The investigations of the Congo Hold-Up leak revealed how the bank was systematically used to launder illicit profits, embezzle public funds, and pay bribes with little oversight and, importantly, how the bank was an access point to move illicit funds through the international monetary system. The leak also raises important questions about how anti-money laundering directives and due diligence rules, the guardrails embedded in the international banking system, failed to curb the movement of the illicit funds.

3.2.1. BGFIBank DRC's Correspondent Banking Relationships

Over the ten years (2011 - 2020) contained in the Congo Hold-Up leak, foreign wire transfers made up a large part of the bank's business. The total volume of foreign transfers was significantly higher than what was transferred domestically. And similar to DRC as a whole, where capital flight was prevalent, foreign transfers flowing out of the country were about three times as large as incoming foreign transfers. In other words, BGFIBank DRC was used to funnel significant amounts of money out of the country, with a total value of outgoing foreign transfers of approximately $1.6 billion over a nine-year period.



VOLUME OF BGFIBANK DRC TRANSACTIONS EXECUTED BY EACH CORRESPONDENT BANK BETWEEN OCTOBER 2010 AND OCTOBER 2019

Without physical locations abroad or licenses to process payments, BGFIBank DRC used correspondent banks to send, receive, and process payments in foreign currencies or to locations abroad. Correspondent banks were even required to process payments in US dollars between domestic Congolese banks. In the early 2010s, many international banks started to reduce their correspondent banking relationships, in particular with banks in the Global South in reaction to stricter AML enforcement at home and risk-benefit assessments. Possibly because only a limited number of partners were now available, BGFIBank DRC routed the vast majority of foreign transfers through two banks: German based Commerzbank and Maltese FIMBank. These two banks were responsible for processing approximately 86% of the total value of foreign transfers for BGFIBank DRC between 2011 and 2016. By far the largest share of the volume of funds transferred internationally by BGFIBank DRC was processed by Commerzbank, which, in total, facilitated international transfers of almost $800 million involving more than 100 countries. Based on the leaked data, Commerzbank was the correspondent bank of choice for 76% of foreign transfers between 2011 until 2016, accounting for 68% of the transferred dollar value. A smaller but relatively constant share of foreign transactions were processed through FIMBank, a smaller international bank located in Malta. In total, FIMBank processed international transactions worth more than $250 million over the nine-year period, 83% of the dollar value being transferred prior to 2016. BGFIBank International, a Paris-based subsidiary of the same parent company as BGFIBank DRC, comes into the picture as the correspondent bank of choice after 2015, though it was already the correspondent bank of choice for a few larger international transfers.

In 2016, international transfers to and from BGFIBank DRC through Commerzbank and FIMBank came to almost a complete stop. In its place, BGFIBank International and BMCE Bank became the correspondent banks of choice and after 2016 almost all international transactions went through BGFIBank International.

Most banks work with a number of different correspondent banks at the same time. The specific correspondent bank varies for individual transactions, with the choice coming down to practical and economic aspects such as the geographic region/time zones, cut-off times, fees, and the liquidity/credits available in the nostro accounts. In addition, the prospective correspondent banks' risk tolerances and AML/KYC requirements may play a role.

BGFIBank DRC used a number of different correspondent banks over the years, in total at least eight correspondent banks appear in the leak.

Respondent banks and their clients can also actively steer payments away from correspondents with stricter controls. In a recent sanctions-evasion example reported by The New York Times, a January 2025 invoice for a shipment to Russia that named Zhejiang Chouzhou Commercial Bank as the company's bank warned payers that the funds could not be received from Standard Chartered, including as an intermediary bank, and not to pay to its Bank of China account if paying from Russia, the UAE or Turkey.[44] Such routing instructions are in themselves a red flag that correspondents should be able to detect.

3.2.2. AML Obligations in the DRC

Efforts to combat money laundering in the Democratic Republic of the Congo remain widely viewed as ineffective. On paper, Congolese banks face a host of obligations to scrutinise the transactions working through their accounts, something the FATF would view as technical compliance. However, the real problems involved enforcement, especially whether the financial system was able to effectively detect and prevent illicit financial flows. A regional assessment conducted under the FATF framework concluded that the DRC falls short of most international standards and shows little practical capacity to detect or prevent illicit financial activity. During the 2010s, financial institutions filed very few suspicious transaction reports, and even large-value transfers flagged to the central bank rarely reached CENAREF, the national financial intelligence unit, for further scrutiny.[45] CENAREF itself had limited operational capacity to effectively scrutinise the banking sector. Ongoing deficiencies ultimately led to the DRC's placement on the FATF grey list in 2022; however, on 30 October 2026, the FATF removed the DRC from the grey list and it is therefore no longer a jurisdiction under increased monitoring.

3.3. SYSTEMIC BREAKDOWN

This section presents case studies of four different international correspondent banks that processed foreign transactions for clients at BGFIBank DRC over a roughly ten-year period. In each case, the international bank neglected its due diligence responsibilities by paying only cursory attention to the alarming irregularities in the documentation accompanying the requested transactions. The consequences of this negligence are severe. Money routed from BGFIBank DRC filled the foreign bank accounts of companies that were sanctioned for having ties to terrorist group Hezbollah, companies directly connected to President Joseph Kabila, and vast money laundering networks spread across the world.

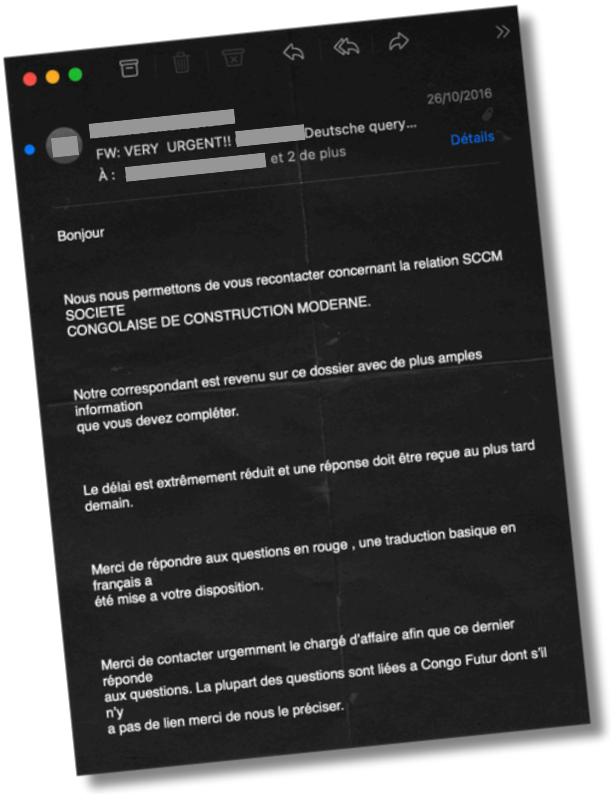
3.3.1. FIMBank

A large, diversified industrial conglomerate, the Congo Futur Group has amassed significant assets in the DRC over the past several decades, including holdings in food trade, logging, and plastic. Yet this business activity has been overshadowed by the sanctions levelled on its founders, brothers Ali and Husayn Tajeddine for helping finance Hezbollah, the Shiite movement designated as a terrorist organisation by numerous countries and international organisations worldwide. Congo Futur is thus one of a notable number of financial networks based in the DRC that have been used to funnel illicit money out of the country. Contacted by Congo Hold-Up consortium partners, Kassem Tajeddine said through his lawyers that he was unable to provide detailed answers because of current and past legal proceedings, while Ahmed Tajeddine and the two men who allegedly de facto control Glory Group's three main companies did not respond.[46] In December 2010, the US Treasury Department hit the Tajeddine brothers with asset freezes and banned any US entities from doing business with Congo Futur; they joined their brother Kassem who was labelled a Specially Designated Global Terrorist by the US in May 2009.

That blacklisting forced Congo Futur to reform its corporate structure, ultimately reconfiguring its assets under a new network of companies called Glory Group. No fewer than 18 Glory Group companies, including their Congo Futur predecessors, operated bank accounts through BGFIBank DRC. These companies executed a significant number of foreign transactions to accounts in the United Arab Emirates, Netherlands, and Malaysia, among other countries.

Throughout this period, transactions initiated by Glory Group companies showed clear signs of potential money laundering, yet these constant red flags failed to raise sufficient alarm among employees either at BGFIBank DRC or one of its correspondent banks, FIMBank, which ultimately executed a majority of these payments. FIMBank blatantly disregarded both its basic due diligence responsibilities as well as explicit warnings from peer financial institutions that the funds coming from Glory Group were suspicious. In the end, Glory Group companies were able to funnel nearly $140 million abroad, in transactions cleared by FIMBank's compliance department.

FIMBank even failed to take necessary action after it received warnings about the Tajeddine brothers from its peer institutions. In 2016, Deutsche Bank alerted FIMBank to the activities of the shell company Société Congolaise de Construction Moderne (SCCM), including both its place within the Glory Group network and its suspicious transactions to Lebanese offshore companies. Contacted by the Congo Hold-Up consortium, SCCM firmly denied the links attributed to it with the Congo Futur network, describing its dealings with Kin Trading (another company allegedly run by Ahmed Tajeddine) as a regular commercial relationship.[47]



Although initially following up to request more information from BGFIBank DRC, FIMBank went ahead and transferred the funds, trusting its Congolese counterpart that nothing was awry.

From 2011 to 2016, FIMBank executed nearly 1,000 transactions worth $140 million from BGFIBank DRC accounts clearly linked to the Congo Futur and Glory Group networks. In practice, this meant a European-regulated bank was facilitating the movement of funds for networks the US Treasury had flagged as Hezbollah financing vehicles. When investigative group The Sentry first reported on these issues, the Maltese bank refused to discuss any individual transactions, citing its obligation to protect client confidentiality,[48] a stance that has allowed it to avoid any real accountability over questionable fund movements linked to BGFIBank DRC. FIMBank also told The Sentry that it maintains the "highest ethical and compliance standards" and abides by all relevant laws and regulations in Malta and the European Union.[49]

3.3.2. Citibank

The Congo Hold-Up leaks also shine troubling light on how correspondent banks failed to uphold their responsibility to scrutinise transactions coming from institutions beyond BGFIBank DRC. During the 2000s, then-president Joseph Kabila established new partnerships with Chinese firms to help execute large-scale and poorly-delivered infrastructure projects. The DRC would grant access to its lucrative deposits of critical minerals in exchange for financing and investment into the country's transportation, health care and the utilities sectors. The most prominent of these initiatives was the mining joint venture Sicomines, formed in 2008 between massive Chinese state-owned enterprises (SOEs) (including China Railway Group Ltd and Sinohydro) and Gécamines, the DRC state-owned mining company. This agreement came under fierce criticism not only for adding billions of dollars of loans to the already indebted Congolese state, but also for providing highly favourable investment guarantees to the Chinese SOEs.

Shortly after launching its extractive activities, Sicomines ran into a clear obstacle: it lacked a stable electricity source. Another joint venture – Sicohydro – was established in 2016, this time to construct a new hydropower dam at Busanga, in southern DRC. However, one of the Congolese partners on this new deal, Congo Management SARL, had again strong ties to the Kabila presidential administration, in particular through its representation in the deal by attorney Norbert Nkulu, who had previously acted as a close Kabila adviser. Moreover, as this infrastructure deal would involve a now notorious shell company, Congo Construction Company (CCC), which over the previous years had funnelled millions of dollars from Sicomines directly into the hands of companies and individuals affiliated with Kabila, his business partners, and even directly to the head of CCC himself, Du Wei.

However, Citibank, the correspondent bank responsible for facilitating the transfer of funds ostensibly to fund the hydropower plant, saw no cause for alarm as the money started flowing. As the correspondent bank for DRC-based Rawbank, where Sicomines held its DRC account, Citibank approved at least $17 million in transfers in the summer of 2016 from Sicomines into CCC's bank account at BGFIBank DRC. The accompanying descriptions of these payments in Swift messages,[50] which amounted to as much as $9 million each, are strikingly vague, simply appearing as "contract costs" (see Exhibit A) or even "payment" (see Exhibit B).

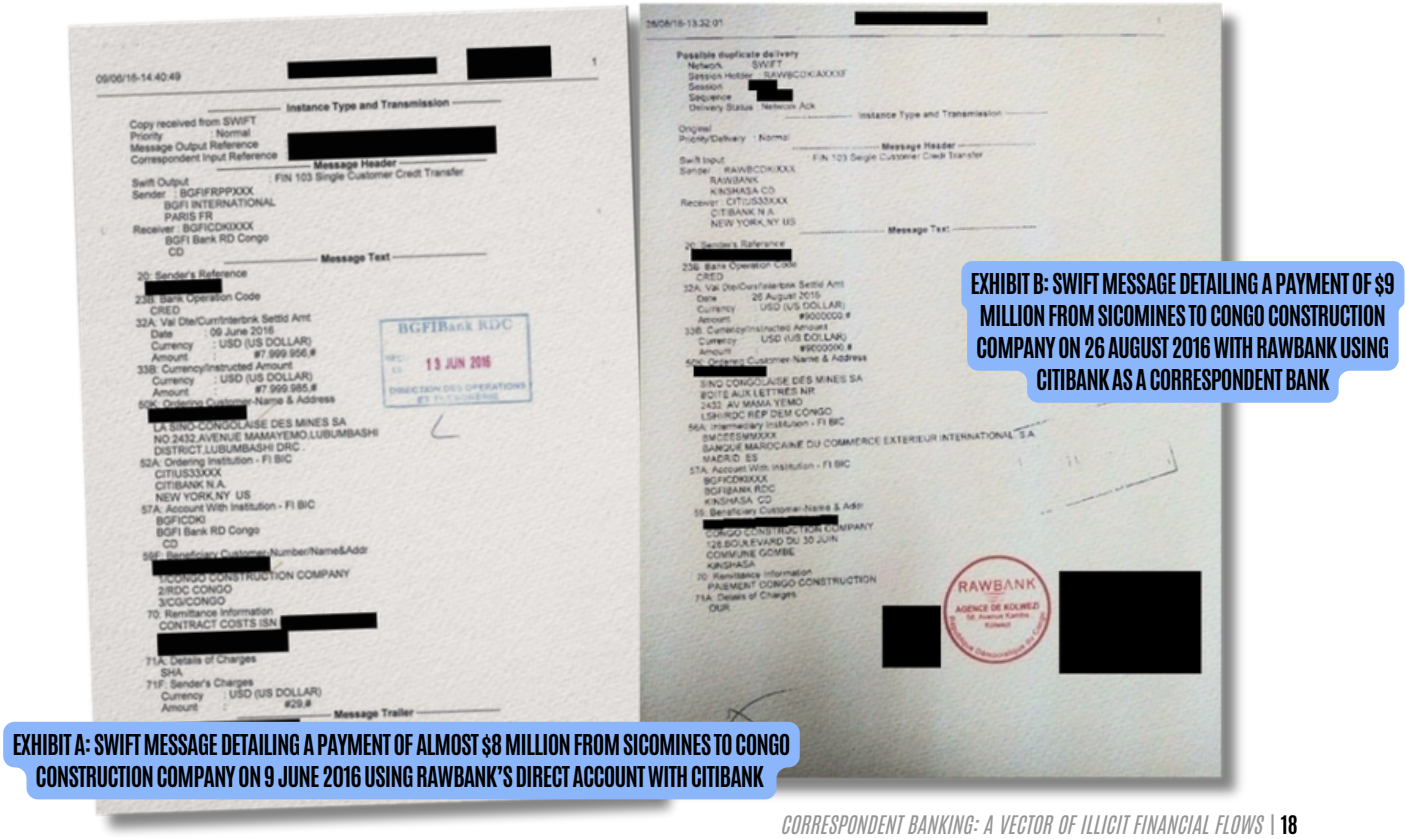


EXHIBIT B: SWIFT MESSAGE DETAILING A PAYMENT OF $9 MILLION FROM SICOMINES TO CONGO CONSTRUCTION COMPANY ON 26 AUGUST 2016 WITH RAWBANK USING CITIBANK AS A CORRESPONDENT BANK

EXHIBIT A: SWIFT MESSAGE DETAILING A PAYMENT OF ALMOST $8 MILLION FROM SICOMINES TO CONGO CONSTRUCTION COMPANY ON 9 JUNE 2016 USING RAWBANK'S DIRECT ACCOUNT WITH CITIBANK

In 2018, an internal auditing team at BGFIBank DRC could not locate the contract supposedly justifying any of these transactions, suggesting that very little if any due diligence occurred on the part of the multiple international banks (Citibank, BMCE Bank, BGFIBank International) that facilitated the transactions. In 2016, Citibank had even approved a much smaller transfer of $100,000 between a different Congolese joint venture and CCC, which had been rejected by a different correspondent bank who questioned its purpose. Citibank apparently was not troubled by its justification as "work expenses".[51]

The Congo Hold-Up leak also clearly shows that none of this money ended up financing infrastructure projects. Instead it was funnelled into an array of companies connected to Kabila. In other words, Chinese enterprises were able to send what appear to be large bribes through the formal banking system directly into the hands of Kabila affiliates, who then appeared to use the funds for their own self-dealing, including paying off loans. Once more it was an international correspondent bank – Citibank – which failed to flag these suspicious transactions that carried no documentation. Contacted by Congo Hold-Up consortium partners, Joseph Kabila and members of his family did not respond, nor did the management of Sicomines or its Chinese shareholders, including China Railway. In a press release dated 29 November 2021, Sicomines formally denied the corruption allegations.[52] Furthermore, in a statement reported by AFP on 25 November 2021 in the Belgian La Libre newspaper, Joseph Kabila's communication service reportedly described the investigation's conclusions as "Kabilabashing" and as an attempt to discredit the former head of state.[53] In December 2021, his lawyers further denied any wrongdoing, calling the reporting "a campaign of defamation, slanderous denunciations, denigrations, and untruths".[54]

3.3.3. BMCE Bank

In 2015, concerns over fraudulent transactions led Citibank to reduce its direct correspondent banking ties with BGFIBank DRC, but it did not exit the relationship outright. Instead, it used a common practice called nesting, when one bank sends payments on behalf of a higher-risk client through another correspondent bank which holds the direct account relationship. BMCE Bank stepped into that intermediary role, allowing Citibank to continue clearing dollar-denominated payments on behalf of BGFIBank DRC while remaining one degree removed from the underlying client.

This nesting arrangement allowed the suspicious transactions to continue with little interruption. In August 2016, Sicomines sent $9 million through Citibank and BMCE Bank en route to Congo Construction Company's (CCC) account at BGFIBank DRC. These transfers were just one part of the broader $25 million in payments that Sicomines ultimately sent to CCC, the latter of which, as we described above, acted as a shell company to funnel money from China to entities linked to former president Kabila.

BMCE Bank itself has acknowledged relying on Citibank for providing its clients like BGFIBank DRC access to international dollar transactions. Here we observe another instance of a large correspondent bank approving large, vaguely described transfers without questioning the contracts supposedly justifying them. Years later, regulators finally took notice. In a resolution from September 2019 (and then published in July 2020), the Bank of Spain sanctioned BMCE Bank (the Madrid-based subsidiary of BMCE Bank of Africa) for serious infringements relating to corporate governance, remuneration policy, organisational structure, and internal control mechanisms.[55]

3.3.4. BGFIBank International

Finally, at the heart of the BGFIBank DRC's connections with the world sat the subsidiary of its parent company, BGFIBank International, headquartered in Paris. From 2016 to 2019, BGFIBank International acted as the correspondent bank for over 12,000 outgoing foreign transactions, or over 40% of the total number by BGFIBank DRC account holders. This sharp increase in coverage was not accompanied by monitoring commensurate with the volume and risk of these transactions.

In total, over one-third of these transactions can be considered suspicious based on investigations carried out under the Congo Hold-Up collaboration and analysis by PPLAAF. These payments totalled $450 million in suspicious funds moved out of BGFIBank DRC and into the international financial system, with BGFIBank International serving as the correspondent bank. Table 1 groups these transactions into six distinct categories. At the top are an enormous number of payments made by legal entities working within Informal Value Transfer Systems, hawala-type networks that can be used to move funds discreetly abroad. BGFIBank International also was heavily involved in approving payments involving the related parties of its Congolese subsidiary.

Table 1

Suspicious Transactions through BGFIBank International

	Num. Transactions (% of total)	Total (mil. USD)
Suspected Informal Value Transfer System Payments that there is a risk may be part of an informal value transfer system (IVTS), the technical term for hawala-like systems, as demonstrated in Section 4.1.4 below on Nizal.	**2,794** (23.2%)	**293.1**
Crime, Conflict and Corruption Allegations Individuals and entities that have been accused of involvement in crime, violence and corruption, whether through credible adverse media, indictments or other reliable sources, as can be seen in Section 4.1.2 on Congo Construction Company below.	**504** (4.2%)	**28.6**
Misconduct Concerning BGFIBank DRC Related Parties Individuals and entities that are, according to the standard accounting definition of the term, substantially linked to BGFIBank DRC itself and its managers and also are known to have directly participated in financial or other misconduct or indirectly participated in such misconduct, such as receiving money from a questionable origin. This can be seen in Section 4.1.1 below on Sud Oil.	**428** (3.6%)	**34.2**
Global Sanctions and Prohibited Activities Individuals and entities that were, during the relevant period, under sanctions, or if not under sanctions when a transaction took place, later information indicates that they were participating in an activity prohibited by the sanction when the transaction took place. This can be seen in Section 4.1.3 on XK Enigma below.	**347** (2.9%)	**38.0**
Misconduct Concerning the Presidential Family Individuals who are part of the presidential family, broadly construed, and any entities linked directly to them who have any direct or indirect relationship with suspected misconduct within the bank, as seen in Section 4.2.1 below on Egal.	**331** (2.8%)	**30.5**
Other Suspected Illicit Financial Dealings Catch-all category for payments that are questionable and problematic. For example we have information that the company appears to be involved in suspicious financial dealings, or offshore companies with accounts at the bank are involved whose transactions were put under scrutiny	**171** (1.4%)	**54.3**
Total	**4,575**	**478.7**

But political corruption also ranks very prominently, especially that related to President Kabila's family, which profited immensely from his eighteen years in power. BGFIBank International was directly involved in the movement of over $30 million in funds from and to entities connected to the presidential administration.

Founded in 2013, Entreprise Générale d'Alimentation et de Logistique (Egal) marketed itself as a "patriotic venture" dedicated to making food affordable for ordinary Congolese citizens by challenging foreign monopolies. Despite this public mission, Egal was secretly controlled by members of former President Joseph Kabila's inner circle, including his personal lawyers Norbert Nkulu and Lunda Banza Wa Seya. The company initially focused on importing horse mackerel from Namibia and was granted exclusive customs and tax exemptions worth millions of dollars. Food prices in the DRC nevertheless continued to rise through Egal's operations, as the company did little to fulfil its main mission of increasing competition in the sector.

More notoriously, investigations conducted both by the Belgian outlet Le Soir and then under the "Congo Hold-Up" collaboration, revealed that Egal received at least $77 million in unexplained transfers, mostly in the form of direct transfers from the Congolese Central Bank. These funds not only helped Egal pay off its staggering debts, but the company also used state funds to finance President Kabila's personal interests, including renovating a luxury yacht and shipping hundreds of wild animals, such as elephants and giraffes, to the president's private zoos. Egal denied having received money from the Central Bank of Congo in its written answers to Congo Hold-Up consortium partners, and stated that it had never been financed by public funds. The company, however, refused to answer the questions from Congo Hold-Up consortium partners, citing the confidentiality of an ongoing judicial investigation.[56]

Acting as a correspondent bank, BGFIBank International played a critical role in enabling the company to transact with the opaque shell companies procuring these goods and services for Kabila. In all, the Congo Hold-Up leak clearly shows that BGFIBank International executed over $34 million in outgoing transactions from Egal from 2015 to 2018.

Many of these payments went to companies run by or associated with two European businessmen and childhood friends: Alain Wan and Marc Piedboeuf. Both have very close ties to President Kabila, appearing in multiple Congo Hold-Up investigations as conduits for the movement of extraordinary sums of money out of the DRC. For example, Egal sent over $1 million to All Ocean Logistics, which had previously received a number of unexplained payments from Kabila-linked firms without any ostensible business purpose. As Faroe Islands lawyer and money-laundering expert Eli Thorsteinsson told PPLAAF: "It looks like money-laundering."

Representtaives of Alain Wan and Marc Piedboeuf refused to answer most of the Congo Hold-Up consortium's questions, describing its information as "mostly false" and its approach as motivated by "a clear intention to harm". They filed a complaint for "slanderous accusation" in Kinshasa against Mediapart, De Standaard and PPLAAF before the publication of the investigation[57]. Much earlier, in 2017, they had defensively told Le Monde that their group did not act on behalf of Joseph Kabila[58]. The managers at All Ocean Logistics did not respond to any of the questions from Congo Hold-Up consortium partners.[59]

Another $2.7 million went to African Trading Maintenance and Development, a shell company registered in Hong Kong with little more than a mailbox. Although African Trading Maintenance and Development claimed to be Egal's "poultry supplier", journalists were unable to find any contracts or customs declarations substantiating this import/export relationship. African Trading Maintenance and Development is reportedly controlled by Alain Wan and Marc Piedboeuf, who, as mentioned above, have refused to answer most of the Congo Hold-Up consortium's questions as they considered the investigation to be "mostly false".[60]

In several cases, the compliance department at BGFIBank International did freeze suspicious payments and demanded identifying information. Warnings were issued to colleagues in Kinshasa that a failure to adhere to US banking laws could lead to both the correspondent bank and its subsidiary being severely punished. Despite these warnings, BGFIBank DRC executives in Kinshasa routinely bypassed safeguards by back-dating documents and creating false trails that successfully deceived compliance officers and auditors at BGFIBank International about the nature of Egal's overdrafts, loans, and contracting relationships. The BGFIBank Group, BGFIBank DRC's parent company, questioned the authenticity of the leaked documents all while stating that it condemned any acts contrary to law and ethics that may have been committed in the past at BGFIBank DRC, possibly with the involvement of its staff. It also said that, beginning in 2018, the bank had conducted an internal audit to identify the methods used to circumvent its internal control procedures.[61]

Part 4:
SYSTEMIC FAILURES

The case of BGFIBank DRC highlights how a respondent bank can be instrumentalised by a kleptocratic regime in order to facilitate the movement of illicit financial flows around the world through correspondent banks. Documents from Congo Hold-Up demonstrate what the actors involved were communicating to each other about these transactions and the level of detail they went into when challenging information gaps. There is also a clear pattern which shows the point that certain correspondent banks no longer wanted to continue their relationship with BGFIBank DRC and which other correspondent banks took over subsequently. However, these issues are not unique to one correspondent bank, one respondent bank, or one country. The issues highlighted by BGFIBank DRC represent the exact dilemmas banks across the world face when dealing with high-risk jurisdictions, a lack of information or changes to the commercial and legal viability of providing correspondent services. This section will deal with some of these challenges, as evidenced by the case study.

4.1. EASY OBFUSCATION AND FAILURE TO CHALLENGE

As correspondent bank systems inevitably flag certain transactions and contact the respondent bank for more answers, it is essential that these questions truly probe into the transaction in line with their regulatory obligations. In the FATF Guidance, there are a series of questions that do not reach the level of CDD but would help to identify whether or not a payment should be reported.[67] Whilst these are presented as suggestions by FATF and not all of them needed to be asked, we found that these questions were barely asked at all, not followed up if no answers were given and not flagged to regulators as suspicious even when the respondent avoided answering the question.

Across the four correspondent banks examined in this paper, a recurring pattern of due diligence failures can be identified once a payment is flagged. In each case, the correspondent bank obtained a response to its query but failed to scrutinise that response for internal consistency, completeness, or alignment with publicly available information. Even when the evidence shows a payment was blocked, we know that the account holders were able to find a way through elsewhere.

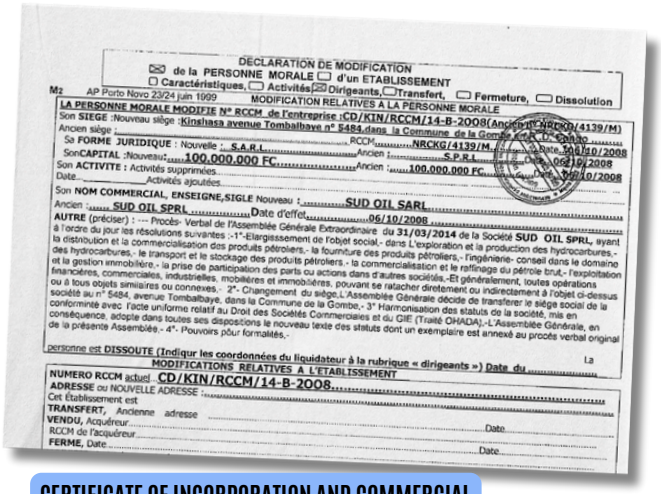
4.1.1. Sud Oil

Documents from Congo Hold-Up demonstrate just how simple it was for those at BGFIBank DRC to avoid scrutiny by BGFIBank International. A small amount more verification would have very easily identified that a payment may have been illicit in nature. In November/December 2013, BGFIBank International asked for the details of a customer that BGFIBank DRC wanted to work with on trade and export finance. On multiple occasions they asked for the details for a Congolese Company called Sud Oil, stating :

> "I would like us to discuss Sud Oil, for which we have no legal information (date of incorporation, shareholding structure, RCCM, etc.). This is important because we cannot proceed with our transaction, which would put us in a difficult position with regard to our client" and "SUD OIL: we absolutely must have the KYC file and the credit file for this entity in order to meet our regulatory requirements."

It is not clear if they ever received confirmation or the transaction continued. This is relevant as three years later, in May 2016, a payment for Sud Oil was flagged by BGFIBank International, who asked BGFIBank DRC simply for the Registre du Commerce et du Crédit Mobilier (RCCM) for Sud Oil.

The RCCM contained the name of the company director, David Ezekiel, the address and the activities of the company. This was attached and the payment went through.



DÉCLARATION DE MODIFICATION

☒ de la PERSONNE MORALE ☐ d'un ETABLISSEMENT

☐ Caractéristiques, ☐ Activités, ☒ Dirigeants, ☐ Transfert, ☐ Fermeture, ☐ Dissolution

AP Porto Novo 23/24 juin 1999 — MODIFICATION RELATIVES A LA PERSONNE MORALE

LA PERSONNE MORALE MODIFIE N° RCCM de l'entreprise :CD/KIN/RCCM/14-B-2008(Ancien N° :NRCKG/4139/M)

Son SIEGE :Nouveau siège :Kinshasa avenue Tombalbaye n° 5484,dans la Commune de la Gombe, R.D. Congo

Ancien siège :

Sa FORME JURIDIQUE : Nouvelle : S.A.R.L. RCCM :NRCKG/4139/M Date 06/10/2008

SonCAPITAL :Nouveau:100.000.000 FC Ancien : S.P.R.L. Date 06/10/2008

Son ACTIVITE : Activités supprimées 100.000.000 FC Date 06/10/2008

Date Activités ajoutées

Son NOM COMMERCIAL, ENSEIGNE,SIGLE Nouveau : SUD OIL SARL

Ancien : SUD OIL SPRL Date d'effet 06/10/2008

AUTRE (préciser) : --- Procès- Verbal de l'Assemblée Générale Extraordinaire du 31/03/2014 de la Société SUD OIL SPRL, ayant à l'ordre du jour les résolutions suivantes :-1°-Elargissement de l'objet social.- dans L'exploration et la production des hydrocarbures.- la distribution et la commercialisation des produits pétroliers.- la fourniture des produits pétroliers,- l'ingénierie- conseil dans le domaine des hydrocarbures.- le transport et le stockage des produits pétroliers.- la commercialisation et le raffinage du pétrole brut,- l'exploitation et la gestion immobilière.- la prise de participation des parts ou actions dans d'autres sociétés.-Et généralement, toutes opérations financières, commerciales, industrielles, mobilières et immobilières, pouvant se rattacher directement ou indirectement à l'objet ci-dessus ou à tous objets similaires ou connexes.- 2°- Changement du siège:L'Assemblée Générale décide de transférer le siège social de la société au n° 5484, avenue Tombalbaye, dans la Commune de la Gombe.- 3° Harmonisation des statuts de la société, mis en conformité avec l'acte uniforme relatif au Droit des Sociétés Commerciales et du GIE (Traité OHADA).-L'Assemblée Générale, en conséquence, adopte dans toutes ses dispositions le nouveau texte des statuts dont un exemplaire est annexé au procès verbal original de la présente Assemblée.- 4°- Pouvoirs pour formalités.-

personne est DISSOUTE (Indiquer les coordonnées du liquidateur à la rubrique « dirigeants ») Date du La

MODIFICATIONS RELATIVES A L'ETABLISSEMENT

NUMERO RCCM actuel :CD/KIN/RCCM/14-B-2008

ADRESSE ou NOUVELLE ADRESSE

Cet Etablissement est

TRANSFERT, Ancienne adresse

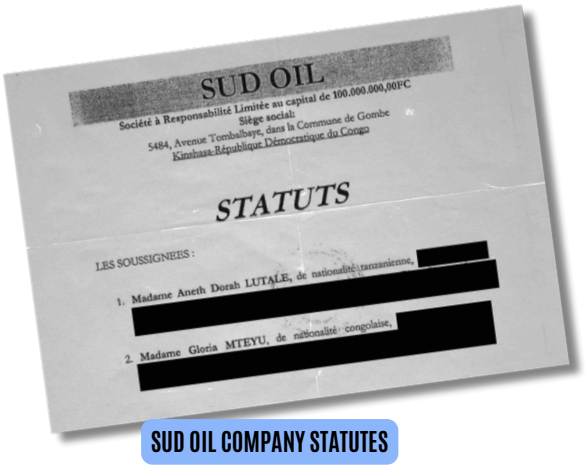
VENDU, Acquéreur Date

RCCM de l'acquéreur

FERME, Date Date

CERTIFICATE OF INCORPORATION AND COMMERCIAL REGISTRATION OR "RCCM" FOR SUD OIL

However, if the bank had simply asked for the company statutes, they would have seen that Sud Oil was owned by President Joseph Kabila's sister, Gloria Mteyu, and his sister-in-law, Aneth Lutale. Gloria Mteyu owned 40% of BGFIBank DRC. Aneth Lutale is the wife of Francis Selemani, Joseph Kabila's adoptive brother and then CEO of BGFIBank DRC.



SUD OIL

Société à Responsabilité Limitée au capital de 100.000.000,00FC

Siège social:

5484, Avenue Tombalbaye, dans la Commune de Gombe

Kinshasa-République Démocratique du Congo

STATUTS

LES SOUSSIGNEES :

1. Madame Aneth Dorah LUTALE, de nationalité tanzanienne, [redacted]

2. Madame Gloria MTEYU, de nationalité congolaise, [redacted]

SUD OIL COMPANY STATUTES

It was also later revealed through Congo Hold-Up what role David Ezekiel and Sud Oil played for the Presidential family when over $90 million in public funds were routed through its accounts:[63]

> "Over half of the stolen funds were withdrawn in cash by Selemani's front-man, Sud Oil General Manager David Ezekiel. Mediapart describes how Ezekiel withdrew $30m in cash from Sud Oil and related companies from May to December 2018, just before Kabila left the presidency in January 2019 after 18 years in power."

Francis Selemani and David Ezekiel did not wish to answer the questions put to them by Congo Hold-Up consortium partners.[64] Joseph Kabila did not answer them either.[65]

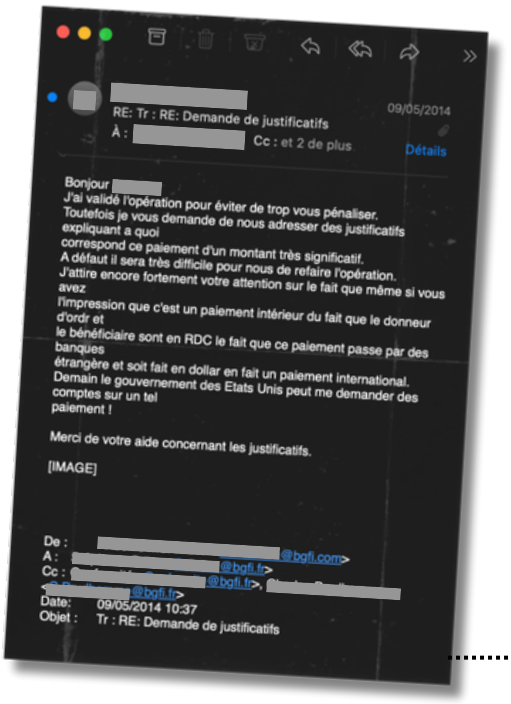
Selemani was also copied into all the emails from November/December 2013. There is no evidence he attempted to provide information on his wife's and his adoptive sister's stakes in Sud Oil, and compliance officers at BGFIBank DRC who knew of these links would likely not have disclosed them without risking their jobs or other harm. Regulators must scrutinise more closely the nature of the questions being asked in these situations, the detail, or lack thereof, in the evidence being requested, and take action against correspondent banks which continue to show a wilful blindness towards evidence which might reveal an illicit transaction.

4.1.2. Congo Construction Company

Another example of a failure to sufficiently challenge a payment that was flagged was in 2014 from a company called Congo Construction Company (CCC). Congo Hold-Up revealed in 2021 that CCC received $55 million from foreign sources apparently intended for Kabila and his entourage through two intermediaries, David Du Wei and Guy Loando. CCC was a shell company established to receive bribes and embezzled public funds to enrich President Kabila. Contacted by the Congo Hold-Up consortium, Guy Loando said that he had acted only as a private lawyer in setting up the company, had played no role in its day-to-day management and had no knowledge of Du Wei's business relations or of CCC's banking operations. Du Wei, on his end, gave no answers[66]. The failure of the correspondent banks that processed foreign currency transfers for BGFIBank DRC (BGFIBank International, Commerzbank and FIMBank) to undertake sufficient due diligence on these payments allowed millions in illicit funds to leave the DRC.

There were opportunities to spot the suspicious transfers but these were missed by each of the correspondent banks. In May 2014, two separate $1 million payments were made to CCC by Société de Gestion de Péage au Congo (SOPECO) ostensibly for the provision of sub-contracting services. SOPECO was under investigation in the DRC for embezzlement in relation to road contracts they received and there is no evidence CCC actually undertook any work for these two payments.[67] SOPECO was owned by Simon Cong, a close associate of CCC's Du Wei and of Guy Loando. When contacted by Congo Hold-Up consortium partners, Simon Cong (Cong Maohuai) denied any embezzlement. In his correspondence with the Congo Hold-Up consortium, he dismissed the inspector general's allegations and claimed he had provided documentation showing that all the money had been spent appropriately. He further specified that SOPECO's two transfers to CCC were for a loan agreement and a gravel supply deal.[68]

The discussions between officers at BGFIBank DRC and BGFIBank International about one of the $1 million payments from 7 May 2014 demonstrate that the correspondent bank did not know CCC or the purpose of the transaction. All they received upon request from the respondent bank was a payment order, a registration form for CCC and their National Identification Number. The correspondent bank allowed the payment through on 9 May knowing this was insufficient and that allowing a payment like this could expose the correspondent bank to liability from authorities in the United States:


RE: Tr : RE: Demande de justificatifs
09/05/2014
À : Cc : et 2 de plus
Détails

Bonjour
J'ai validé l'opération pour éviter de trop vous pénaliser.
Toutefois je vous demande de nous adresser des justificatifs expliquant a quoi
correspond ce paiement d'un montant très significatif.
A défaut il sera très difficile pour nous de refaire l'opération.
J'attire encore fortement votre attention sur le fait que même si vous avez
l'impression que c'est un paiement intérieur du fait que le donneur d'ordr et
le bénéficiaire sont en RDC le fait que ce paiement passe pàr des banques
étrangère et soit fait en dollar en fait un paiement international.
Demain le gouvernement des Etats Unis peut me demander des comptes sur un tel
paiement !

Merci de votre aide concernant les justificatifs.

[IMAGE]

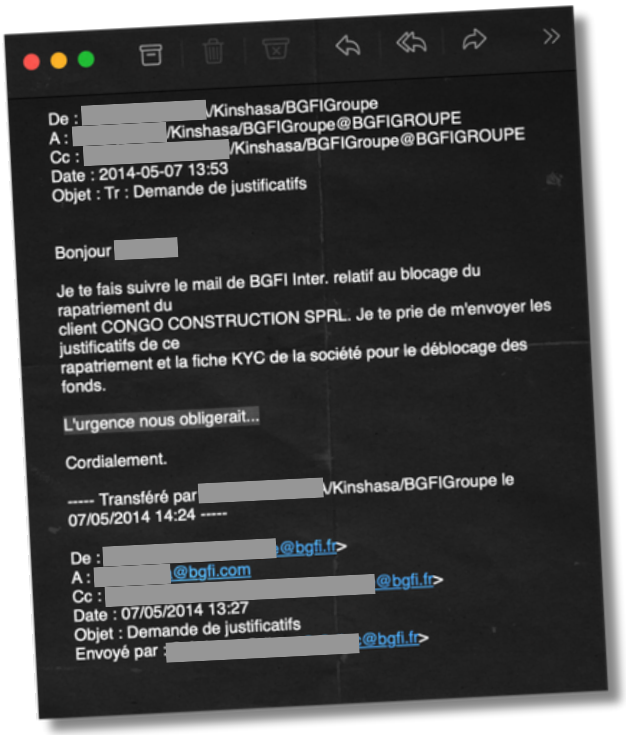
De :
A :
Cc :
Date: 09/05/2014 10:37
Objet : Tr : RE: Demande de justificatifs

"I approved the transaction to avoid penalising you too heavily. However, I ask that you send us supporting documentation explaining what this very large payment is for.

Otherwise, it will be very difficult for us to reprocess the transaction. I would like to strongly emphasise that even if you believe this is a domestic payment because the payer and the payee are in the DRC, the fact that this payment goes through foreign banks and is made in US dollars makes it an international payment.

Tomorrow, the US government could hold me accountable for such a payment!"

The discussion between the client relationship manager and the compliance team at BGFIBank DRC highlights why this lax due diligence was significant. The compliance officer requests the information and says "[t]he urgency would force us to…" with little explanation. The manager then responds that the client "receives several remittances each month in connection with his work (mining construction)" and "[s]ince the client is currently out of the country, the supporting documents will be available upon his return next month". There is clearly a sense that the situation is unusual and the correspondent bank may not consider the documents submitted as sufficient.



De : [redacted]/Kinshasa/BGFIGroupe
A : [redacted]/Kinshasa/BGFIGroupe@BGFIGROUPE
Cc : [redacted]/Kinshasa/BGFIGroupe@BGFIGROUPE
Date : 2014-05-07 13:53
Objet : Tr : Demande de justificatifs

Bonjour [redacted]

Je te fais suivre le mail de BGFI Inter. relatif au blocage du rapatriement du
client CONGO CONSTRUCTION SPRL. Je te prie de m'envoyer les justificatifs de ce
rapatriement et la fiche KYC de la société pour le déblocage des fonds.

L'urgence nous obligerait...

Cordialement.

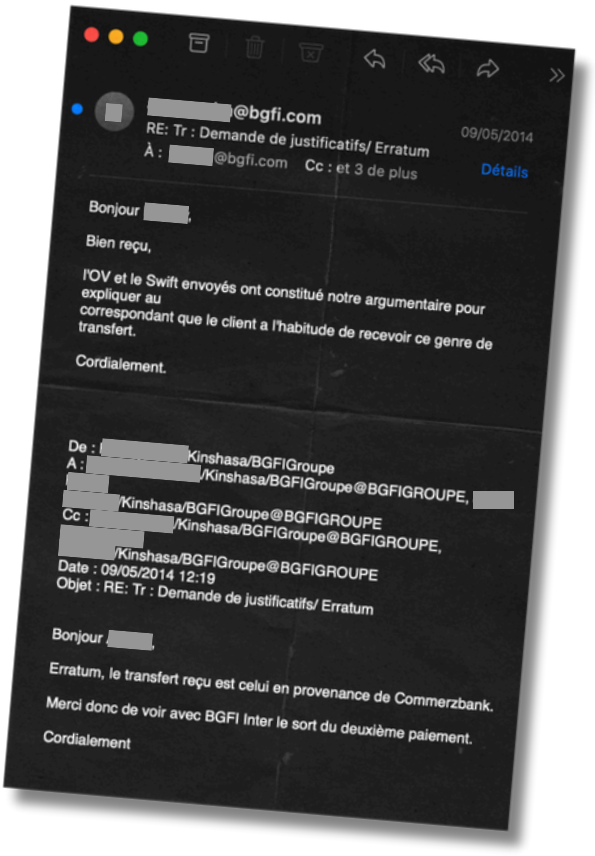
----- Transféré par [redacted]/Kinshasa/BGFIGroupe le 07/05/2014 14:24 -----

De : [redacted]@bgfi.fr>
A : [redacted]@bgfi.com
Cc : [redacted]@bgfi.fr>
Date : 07/05/2014 13:27
Objet : Demande de justificatifs
Envoyé par : [redacted]@bgfi.fr>

In the next two days, it is clear from email correspondence that a second $1 million payment processed through Commerzbank was allowed through without any issues. This is then used by the respondent bank to explain to the correspondent bank that this was an entirely normal transfer - "the OV [payment order] and Swift messages we sent formed the basis of our explanation to the correspondent that the client is used to receiving this type of transfer".

At no point is there an attempt to understand the rationale of the transaction or the business relationship. Nor is there any attempt to actually scrutinise CCC. While the conduct of both BGFI entities is concerning, it is even more problematic that there does not seem to be any concern at all by Commerzbank.

Two years later, in June 2016, BGFIBank International validated an $8 million payment issued by Sicomines to CCC, the justification for which was only "contract costs" (Exhibit A in Section 3.2.2). Clearly no lessons were learnt and sufficient additional supporting documents were not obtained. CCC, Du Wei and Loando had no legitimate experience in this area to justify these deals and there is no evidence a contract was sent as evidence in any case. Once again, it is clear that the correspondent banks did not fulfil their obligations to properly scrutinise the clear red flags around CCC. Commerzbank declined to comment on the transactions and emphasised its overall efforts to conduct appropriate due diligence and abide by all applicable laws and regulations.



[redacted]@bgfi.com
RE: Tr : Demande de justificatifs/ Erratum
09/05/2014
À : [redacted]@bgfi.com Cc : et 3 de plus
Détails

Bonjour [redacted],

Bien reçu,

l'OV et le Swift envoyés ont constitué notre argumentaire pour expliquer au
correspondant que le client a l'habitude de recevoir ce genre de transfert.

Cordialement.

De : [redacted]/Kinshasa/BGFIGroupe
A : [redacted]/Kinshasa/BGFIGroupe@BGFIGROUPE, [redacted]
[redacted]/Kinshasa/BGFIGroupe@BGFIGROUPE
Cc : [redacted]/Kinshasa/BGFIGroupe@BGFIGROUPE,
[redacted]/Kinshasa/BGFIGroupe@BGFIGROUPE
Date : 09/05/2014 12:19
Objet : RE: Tr : Demande de justificatifs/ Erratum

Bonjour [redacted],

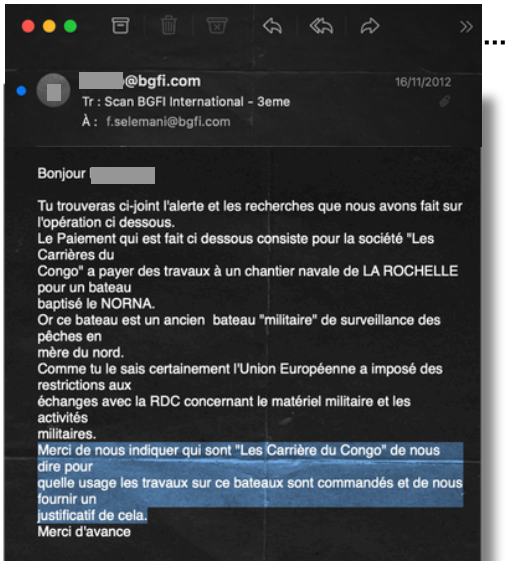
Erratum, le transfert reçu est celui en provenance de Commerzbank.

Merci donc de voir avec BGFI Inter le sort du deuxième paiement.

Cordialement

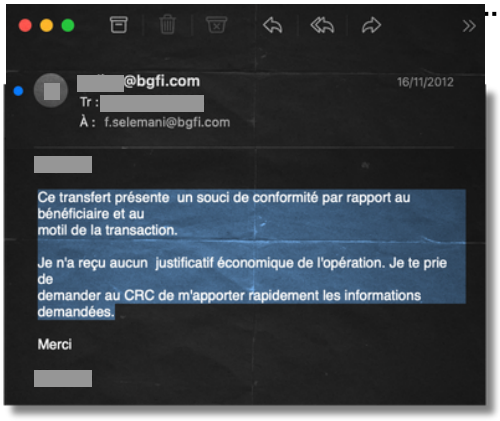
4.1.3. XK Enigma

When a correspondent bank blocks a transaction for a potential sanctions violation and asks for further information, a payment that is then simply cancelled within hours, rather than justified, should itself be treated as a red flag and reported to the relevant authorities. In November 2012, BGFIBank International questioned BGFIBank DRC about a flagged payment of $767,500.



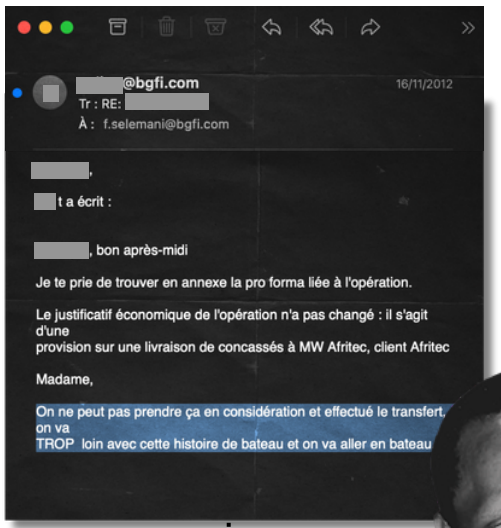
"You will find attached the alert and the research we have done on the operation below. The payment below is for the company "Carrières du Congo". It is to pay for the ship Norna at a shipyard at La Rochelle. However, this boat is a former "military" vessel used for fisheries surveillance in the North Sea. As you know, the EU imposed restrictions on exchanges of military goods and activities with the DRC. Please clarify what the "Carrières du Congo" and for what purpose was the work on this boat commissioned and to provide proof for this"

Emails between the compliance officers and the client relationship team at BGFIBank DRC demonstrate the trouble this email created. The email below shows a conversation where a compliance officer is given minutes to provide a green light to the correspondent bank in Paris but raises concerns:



"This transfer presents a compliance concern regarding the beneficiary and the reason for the transaction. I have not received any economic justification for the transaction. Please ask the CRC [Client Relationship Centre] to provide me quickly with the requested information"

They are told the payment is for "delivery of crushed stone/aggregate to MW Afritec" by the CRC and the manager follows up to say "we are going TOO far with this boat story, and we're going to end up going nowhere with it". The compliance officer responds that the CRC is confusing two transactions, and that they "don't have any economic justification for the transfer, and [they] have no explanation to give the correspondent bank for this transfer, nor any document". Minutes later, the CRC contacts the correspondent bank directly and cancels the transaction. Within the next two hours, all of this detail on one cancelled transaction is forwarded directly to Francis Selemani, the CEO of the Bank.





If BGFIBank International did file a suspicious transaction report, there is no indication that it was acted upon. The ship in question, Norna, received a luxury refit and was reborn as XK Enigma.[69] XK Enigma turned out to be owned by MW Afritec, and owned by Joseph Kabila and two of his proxies.[70] Either the correspondent bank didn't report this suspicious transaction to TRACFIN, France's financial intelligence unit, or TRACFIN and the competent authorities did not do enough to investigate the transaction. This demonstrates that even when the internal risk based evaluation works and a transaction is stopped, the potentially illicit activity it relates to cannot be prevented unless the transaction is reported externally and the competent authorities investigate.

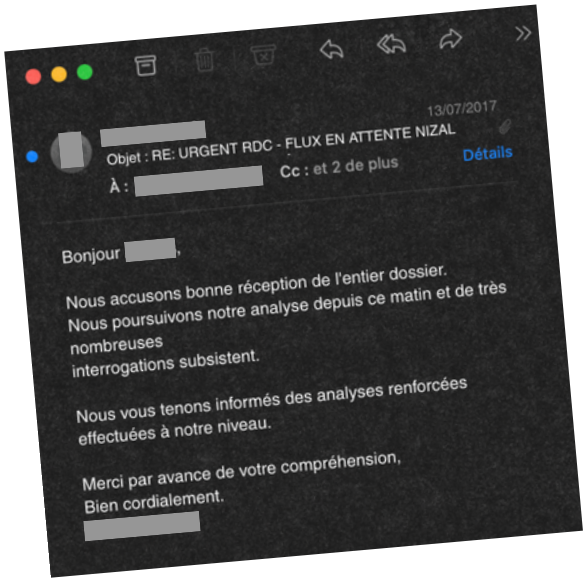
4.1.4. Nizal

Compliance systems also need to be able to identify suspicious transactions based on the nature and frequency of transactions made from specific entities, not simply because a name has triggered a red flag. Congo Hold-Up revealed the existence of a network composed of several dozen institutions and one-person companies that, between 2015 and 2019, received hundreds of millions of dollars in cash and transferred them via wire transfers abroad. The correspondent banks failed to prevent these illicit financial flows. Despite being contacted by Congo Hold-Up consortium partners, Nizal's manager did not respond, and the person named as its owner could not be reached.[71]

This network of companies is similar to a hawala network. The term 'hawala' is associated with a centuries-old money transfer mechanism that operated extensively in South Asia, the Middle East and Africa. It is referred to more broadly as "hawala and other similar service providers" or HOSSPs in AML/CFT typology as it is a way of transacting rather than a specific system. Money transmitters, particularly with ties to specific geographic regions or ethnic communities, arrange for the transfer and receipt of funds or equivalent value in different currencies and settle through trade, cash, and net settlement over a long period of time.[72]

Across the data we can see more than 1,400 transactions from one company, Nizal, almost all going through either BGFIBank International or BMCE Bank as the correspondent bank. These transactions totalled almost exactly $140 million between June 2016 and July 2017 with Nizal only having been established months earlier. Nizal received large cash deposits constituting the bulk of its funds and this corresponded to almost exactly a one-to-one ratio with foreign transfers out.

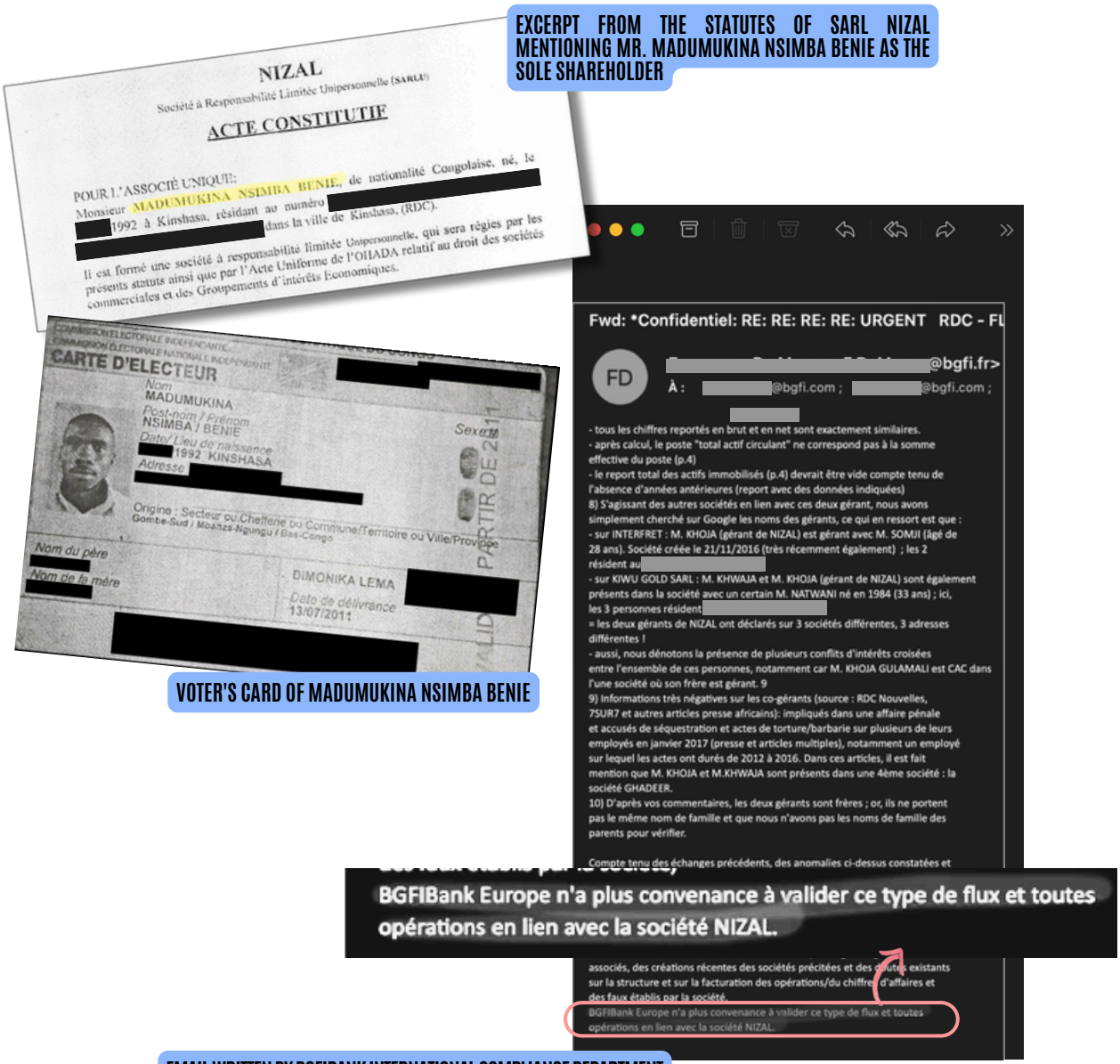
For more than a year these transactions continued to be made with little challenge until the respondent bank was asked by BGFIBank International for a complete KYC file ("articles of association, extract from the trade register, invoices, lists of directors and beneficial owners, etc") and notified them Nizal had been placed under monitoring ("Please also note in advance that the customer Nizal has been placed under monitoring and will be subject to enhanced monitoring in view of the country risk, the diversity of its activities and the goods concerned, and finally the failure to provide justification for some of these transactions during our ex-post checks").



It took more than two weeks for the respondent bank to return with the identity of the beneficial owner and the company statutes. It turned out that the beneficial owner was a 24-year-old with little public presence, and the correspondent bank immediately suspected he was a nominee.

It was only when the real individuals behind the company and the hawala network were named that the correspondent bank started to develop serious concerns and decided to block all payments related to Nizal. The compliance officer at BGFIBank International raised a lot of red flags, including articles according to which the owners/managers of Nizal were accused of torture.

However, by this point, almost $140 million had already left the DRC and filtered throughout the hawala network. Despite the fact compliance officers at BGFIBank International had on multiple occasions failed to receive justification for previous transfers, it took more than a year for this channel for illicit financial flows to be blocked. A more proactive system could have prevented tens of millions from being lost.



EXCERPT FROM THE STATUTES OF SARL NIZAL MENTIONING MR. MADUMUKINA NSIMBA BENIE AS THE SOLE SHAREHOLDER

VOTER'S CARD OF MADUMUKINA NSIMBA BENIE

EMAIL WRITTEN BY BGFIBANK INTERNATIONAL COMPLIANCE DEPARTMENT BLOCKING ALL NIZAL TRANSACTIONS DATED 25 JULY 2017

4.2. INVOICES AS PROOF

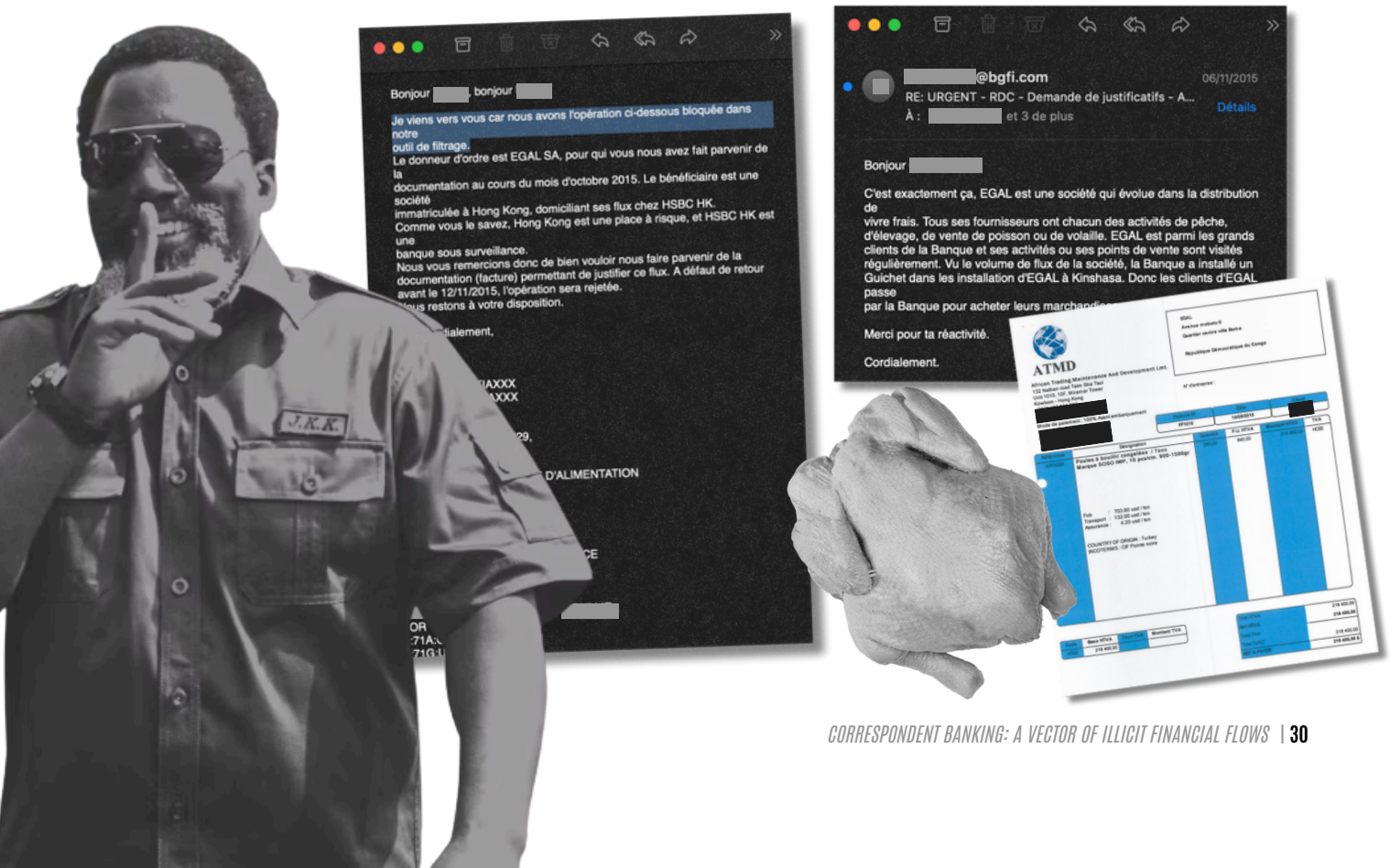
On a number of occasions a simple invoice was all that was required to convince a correspondent bank to approve a payment after serious questions were asked about the jurisdictions involved and incorrect payment details. These red flags should have triggered further questions on each occasion beyond a simple invoice. Even worse, sometimes the details on those invoices were not even verified. The receipt of an invoice, without further scrutiny, should not be sufficient for a compliance official to approve a flagged transaction.

4.2.1. Entreprise Générale d'Alimentation et de Logistique

On multiple occasions BGFIBank International and other correspondent banks flagged payments by Entreprise Générale d'Alimentation et de Logistique (Egal), a tax-exempt company formed in 2013 by Belgian businessmen close to Joseph Kabila, Marc Piedboeuf and Alain Wan (see Section 3.3.4).

The Lumumba Papers and Congo Hold-Up leaks revealed that in 2013 Egal received $43 million from the DRC Central Bank which was used as slush funds for the Kabila family.[73] Albert Yuma, then member of the Central Bank of Congo's Board and chair of its Audit Committee, was also a board member of Egal at the time. He was contacted by Congo Hold-Up consortium partners in 2021 but did not respond.[74] Yuma had previously told journalists that the Central Bank had not sent any funds to Egal when, in November 2017, an Organised Crime and Corruption Reporting Project story[75] had already shown where some of the $43 million went. One company was connected to Wan and Piedboeuf, African Trading Maintenance and Development Limited (ATMD - see Section 3.3.4).

Egal made nearly 90 payments totalling more than $18 million to African Trading Maintenance and Development Limited between 2013 and 2017. In November 2015, a $120,000 payment was blocked as the company was in Hong Kong and the recipient bank (HSBC HK) was under monitoring. The correspondent bank itself acknowledged that the manager is Belgian National "Raphael Piedboeuf" but failed to ask any more questions about the shared surname between individuals at the two entities.

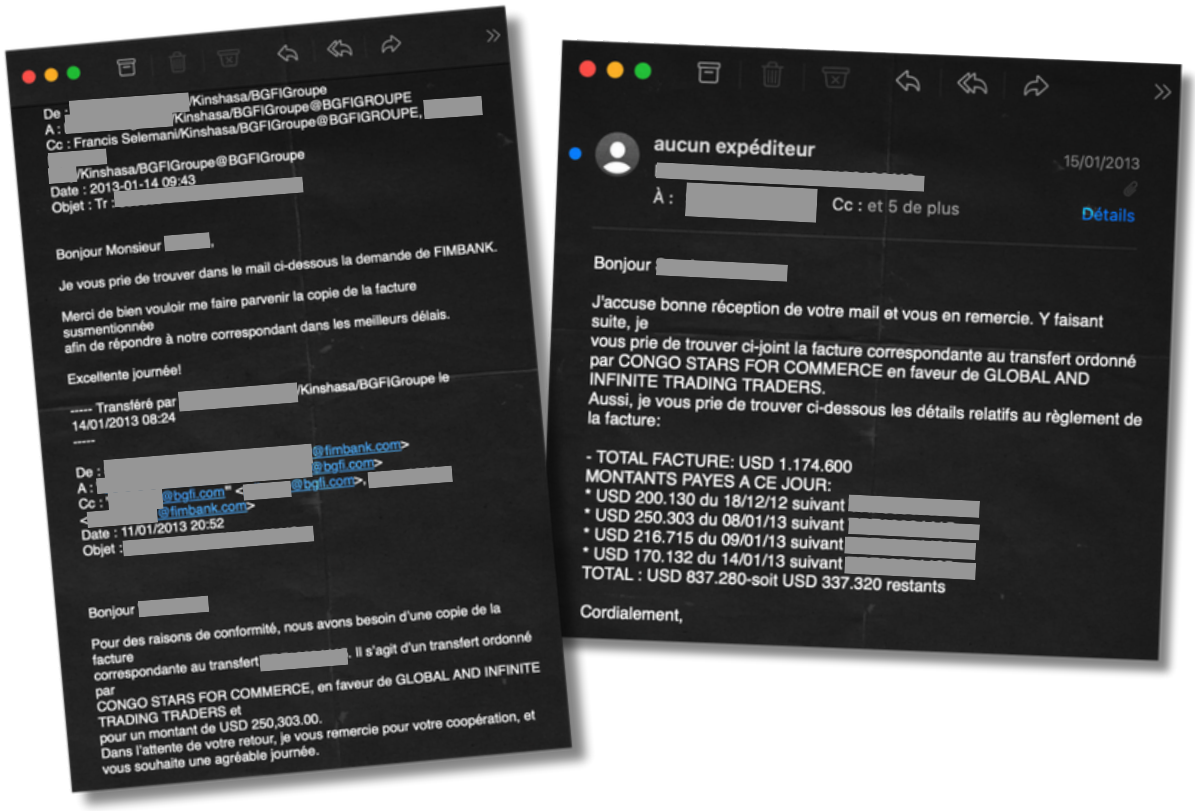


4.2.2. FIMBank

This issue was not unique to BGFIBank International. A report by the Sentry in 2021[76] has already shown how BGFIBank DRC sent a fake invoice to its correspondent bank, FIMBank in Malta, in order to justify a transaction involving Congo Construction Company (4.1.2. above). FIMBank asked for the underlying contract and, when a basic two-page contract was provided, the transaction was cancelled as the response window had closed. But there were other instances where it did not.

Most lapses involved missing, incomplete, and potentially falsified documentation that should at a minimum have caused concern among FIMBank employees and been grounds for refusing to execute transactions. In 2013 and 2014, FIMBank approved several large transactions from a Congo Futur-linked company General Trade Company to Meat Plus BV, a meat exporter from the Netherlands. However, in each case, the accompanying invoices had serious deficiencies that went unnoticed. For example, FIMBank never stopped to question why the dollar amount listed on one invoice from General Trade Company in February 2013 did not match the total listed on the transaction amounting to more than $216,000.

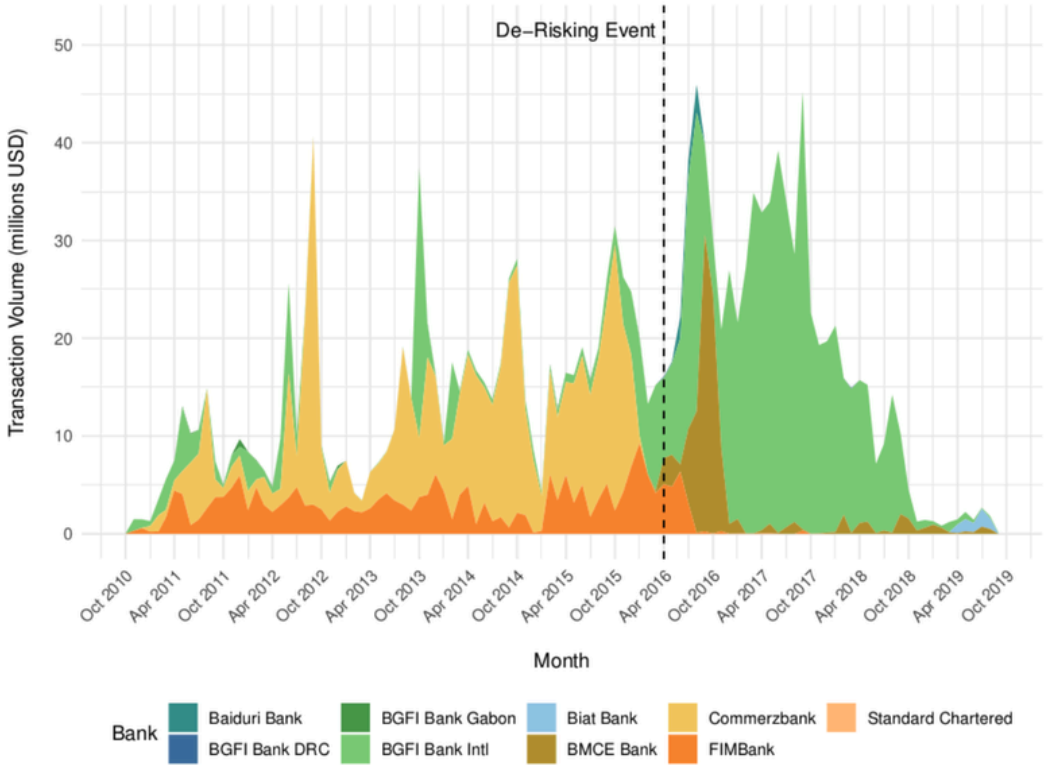
At times FIMBank employees did identify problems in invoices coming from BGFIBank DRC and suspended payments until proof of payment was provided or other inconsistencies were addressed. However, the information in the Congo Hold-Up leak clearly shows that FIMBank employees failed to sufficiently verify the follow-up documents they were given in response. For example, in November 2011, BGFIBank DRC initially did not provide any invoice for a $152,000 transaction from Congo Futur-linked Congo Stars for Commerce to the same meat exporter from the Netherlands, Meat Plus BV. When FIMBank held up the payment, an invoice was finally shared, and even though its numbers once again did not align with the transaction amount, FIMBank ultimately cleared it. A similar case arose in 2013 when again FIMBank re-requested invoices for another transaction by Congo Stars for Commerce, only to later fail to scrutinise them for having correct amounts, dates, or descriptions of the goods and services. Yet again those transfers, together worth over $1 million, were ultimately approved.



4.3. DE-RISKING AND SUSPICIOUS TRANSACTIONS

By the end of 2016, several of BGFIBank DRC's main correspondent banking partners appeared to sever their agreements. As first uncovered in reporting from the Congo Hold-Up, compliance officers at Commerzbank in early 2016 were blocking suspicious foreign transfers out of BGFIBank DRC unless additional documentation was provided. This came at a time when Commerzbank was reevaluating many of their correspondent banking relationships in the wake of its 2015 settlement with US authorities over AML and sanctions failures, including "failing to conduct due diligence on its foreign correspondent accounts, and willfully failing to file suspicious activity reports".[77] Ultimately the suspicious foreign transfers were never processed by Commerzbank and led to the termination of the correspondent banking relationship between Commerzbank and BGFIBank DRC. While in 2015, Commerzbank processed almost three quarters of the foreign transactions for BGFIBank DRC, by spring of 2016, it stopped processing any international transfers originating or being sent into the bank. By April 2016, Commerzbank had effectively 'de-risked' BGFIBank DRC. In its annual report for 2016, published in March 2017, Commerzbank explained that it had significantly decreased the number of correspondent banking relationships in 2016. The bank noted that in addition to cost-benefits, 'compliance standards played an important role'.[78]

Nevertheless, despite the termination of the correspondent banking relationship by Commerzbank, the outflow of suspicious funds did not slow, let alone stop. More importantly, foreign transfers by cash heavy accounts, suspicious for illicit behaviour, continued at a similar pace, now processed by substitute correspondent banks. That continuity is in large part due to the role of BGFIBank International. From 2016 onwards, BGFIBank International executed approximately 71% of all outgoing transactions from its Congolese subsidiary, a roughly 58 percentage point increase on the previous six-year-period. This trend is neatly illustrated in the graphic below, where we see the substitution of Commerzbank and FIMBank in early 2016, and the two other European banks (BGFIBank International and BMCE Bank) continue to process a large volume of outgoing transactions from BGFIBank DRC.



VOLUME OF BGFIBANK DRC TRANSACTIONS EXECUTED BY EACH CORRESPONDENT BANK BETWEEN OCTOBER 2010 AND OCTOBER 2019

Commerzbank's withdrawal helps demonstrate one of the central flaws in de-risking as an anti-money laundering tool: it addresses institutional exposure, not illicit financial flows. The suspicious funds did not stop; they simply moved through another correspondent bank within the same corporate family. BGFIBank International stepped in almost seamlessly, absorbing the transaction volume Commerzbank had refused to process. In effect, the compliance concerns that led one bank to walk away were answered not by greater scrutiny, but by a related entity willing to look the other way. This pattern is neither specific to BGFIBank DRC nor to kleptocracy. In June 2025, Bank of America closed, without public explanation, the dollar account of Zhejiang Chouzhou Commercial Bank. Soon afterwards, Chouzhou opened new dollar accounts at Citibank and Standard Chartered, which remained open as of October 2026, and it continued to provide dollar access to dozens of banks, including in countries with close economic ties to Russia.[79] The banks that commented told the newspaper that they monitor correspondent activity and report suspicious transactions. As with Commerzbank's exit from BGFIBank DRC, the departure of one correspondent displaced the risk rather than removing it.

Whilst BGFIBank DRC is a story of a captured financial institution, it also highlights the significant risk when a subsidiary or group financial institution takes on the role of sole correspondent bank when others in the market withdraw due to a high-risk respondent bank. Regulators must be aware of these situations and carefully assess whether the correspondent bank which continues to provide services, especially if they are a related entity, has the capacity and the independence to manage the risk.

Part 5:
Recommendations

5.1. TO REGULATORS AND LAW ENFORCEMENT AUTHORITIES

BGFIBank DRC provides an instructive example of what a respondent bank under state capture looks like. The number of transfers which can be categorised as 'suspicious' and should have been flagged to regulators was significant. Risk-appetite is a problem on both ends of the scale. One correspondent bank can decide the cost of compliance is too high, which leads to financial exclusion for citizens; however, if another correspondent bank has no concerns about the risk, potentially because they themselves are captured in some way, then the risk of unchecked illicit financial flows is significant. A necessary part of the solution is to heavily penalise those correspondent banks which continue to flout the rules.

However, it cannot be left to banks alone. For years it has been clear national-level regulators are not doing enough and greater oversight is needed. Regulators have to be more involved to monitor what correspondent banks are doing and whether they are maintaining a high-quality human analysis of flagged transactions.

- Require national supervisors to conduct periodic thematic reviews of correspondent banking relationships with high-risk jurisdictions.
- Ensure that supervisory reviews assess how correspondent banks deploy new monitoring technologies, including AI, so that efficiency gains translate into better-quality human review of alerts rather than reductions in compliance staff.
- Monitor de-risking decisions in real time, proactively assessing who is taking over and whether that institution is equipped to manage the risk, with particular scrutiny when a related entity steps in as sole correspondent bank. The risk profile of the respondent bank should be taken into account. This should include tracking whether a respondent exited for financial-crime reasons promptly obtains replacement accounts at other correspondents.
- Where a respondent bank shows signs of state capture, such as PEP ownership, politically exposed directors, or government-linked shareholding, correspondent banks should be required to apply heightened verification.
- Ensure full compliance with FATF Recommendation 13, with supervisors examining correspondent banks' end-to-end processes rather than simply whether respondents pass international standards.
- Require enhanced due diligence for banks with known political entanglements, and take the quality and independence of local auditors into account in country risk assessments.
- Improve coordination and collaboration between enforcement authorities to ensure information on problematic correspondent banking practices is shared in a timely and effective manner.
- Strengthen whistleblower protection in the banking sector, explicitly covering compliance officers and staff of respondent banks, and ensure that supervisors act on whistleblower reports.

- Set fines sufficiently large that they disincentivise the behaviour.
- Investigate and possibly prosecute senior managers of the correspondent bank if they had knowledge of, or were complicit in, illicit activities.
- Set up clear guidelines to force the referral to law enforcement where illicit behaviour is frequent and consistent, to assess whether the correspondent bank's acts have reached the criminal threshold for facilitation of financial crimes.

5.2. TO CORRESPONDENT BANKS

Correspondent banking is a massive financial machine through which the vast majority of cross-border payments flow. Banks should use this position to detect and stop illicit flows. Correspondent banks should act as committed partners for the health of the financial institutions they work with. That means avoiding de-risking without engagement. Standard Chartered's Correspondent Banking Academy, set up in 2015, offers one model: it works with respondent banks to build their financial crime controls, and by 2019 reported reaching over 1,200 respondent banks in more than 70 countries.

In practice, correspondent banking is seen as commercially viable as long as the cost of compliance isn't too high given the margins on each transaction. If a respondent bank becomes too risky, the cost of compliance doesn't justify the fee they charge per transaction, and the financial institution leaves the arrangement. Long term this leads to financial exclusion for high-risk countries. We can't expect banks to manage this balance of risk/reward by attempting to bring down the cost of compliance without lighter-touch monitoring or less oversight. Recent developments in the industry on the use of artificial intelligence have demonstrated a way in which this could occur. HSBC has reported that an AI-based monitoring system it deployed led to 60% fewer false positives being flagged for human analysis and two to four times more discovery of financial crimes. They are not alone as there is reporting on Citigroup and JPMorgan Chase implementing similar systems. This reduction in time would likely result in significant saving on time spent analysing false positives and a greater ability for correspondent banks to spend the time investigating thoroughly flagged payments by respondents which have a higher likelihood of being illicit in nature.

The potential for better compliance is real, but the emphasis needs to be on improving the human part of it. The goal should be to seize technological improvements for more thorough human analysis, so that compliance teams do their job better as technology is implemented, which makes compliance more effective.

- When a flagged transaction generates a response from the respondent bank, banks should be verifying respondent documentation for internal consistency and against public registries and prior transaction patterns, not treating receipt of a document as proof of its content.
- AI-driven transaction monitoring should be paired with mandatory human review of every remaining flag.
- Rather than severing ties abruptly, correspondent banks should provide respondent banks with structured roadmaps for compliance improvements and, where feasible, technical support.
- When a correspondent bank decides to de-risk a relationship for financial-crime reasons, it should be required to notify its home-country supervisor, which should share this information with the respondent bank's supervisor.

- Correspondent banks should monitor transactions dynamically, and freeze those lacking an economic rationale or with vague justifications pending documentation.
- Correspondent banks should monitor indicators of disproportionate activity at respondent banks, such as cross-border payment volumes far exceeding the respondent's balance sheet or an unusually large number of downstream banks relying on a single respondent for dollar access.
- Correspondent banks should evaluate the independence and quality of their respondents' auditors, especially in high-risk countries.
- Banks should keep escalation chains documented and auditable.

5.3. TO CIVIL SOCIETY AND MEDIA

The centrality of correspondent banking at the heart of the global financial infrastructure through which the vast majority of cross-border payments flow clearly gives civil society and investigative journalists both a moral and a practical stake in how the sector is policed. Because correspondent banking is technical and opaque by design, effective scrutiny requires civil society organisations to build genuine expertise in its mechanics, such as nostro/vostro relationships, KYC pass-through and de-risking patterns, rather than treating it as a black box beyond their reach. Investigative journalists, in turn, have a role in documenting specific affairs as they unfold, as the BGFIBank DRC case illustrates, translating supervisory failures into public record where regulators stay silent. Where banks or regulators fall short of these responsibilities, civil society and the press must be prepared to hold them to account through public reporting, litigation support, sustained pressure on supervisors to act, and where regulators do not publish their findings proactively, pressing for access through freedom-of-information mechanisms.

5.4. TO AUTHORITIES IN RESPONDENT COUNTRIES, INCLUDING THE DRC

The BGFIBank DRC case began with the capture of a domestic bank and the failure of domestic oversight (Section 3.2.2). Lasting solutions cannot rest on correspondent banks and foreign supervisors alone.

- The Banque Centrale du Congo and CENAREF should ensure that large-value and suspicious transfers reported by banks are systematically transmitted to and analysed by CENAREF, and should publish annual statistics on reports received and disseminated.
- Fit-and-proper and beneficial ownership checks should be strengthened for bank shareholders and senior managers who are politically exposed persons or their relatives.
- Congolese judicial authorities should investigate the transactions revealed by Congo Hold-Up and cooperate with French, Belgian and other authorities through mutual legal assistance.
- A dedicated whistleblower protection law should protect employees of financial institutions, including compliance staff, who report wrongdoing, in line with international standards.

CONCLUSION

Correspondent banking is at the heart of the international financial system. The vast majority of cross-border payments flow through correspondent banks and the system has been designed so that, morally and legally, it allows for regulation both by correspondent banking and of correspondent banking: correspondent banks are expected to scrutinise the respondent banks and transactions they process, and supervisors are expected to monitor whether they are doing so effectively. In principle, this should make correspondent banking one of the most effective means of detecting illicit financial flows, but in practice the system is deeply flawed. The BGFIBank DRC case illustrates this,, with suspicious transfers passing through correspondent accounts for years, concerns raised by compliance staff being overridden, and the risk simply moving to another institution when a correspondent bank decided to de-risk.

Fixing this matters for the stability of the financial system, for the public interest and for the fight against illicit financial flows around the globe. . There are many opportunities to do so, whether those flagged in this report, those raised by the preliminary investigation opened in France against a correspondent bank following the Congo Hold-Up revelations , or the many more which are not covered here. Those flagged in this report include stronger supervision of correspondent banking relationships, closer scrutiny of respondent banks showing signs of state capture, better information-sharing between banks and regulators, the use of technology to improve the quality of compliance, stronger whistleblower protection, and greater transparency for civil society and media and action by authorities in respondent countries.

Because correspondent banking is so large and so central to the global economy, even modest improvements in how it is supervised would significantly narrow the space available to kleptocrats and money launderers, while preserving access to the international financial system for the countries that need it most.

ANNEX
FATF GUIDANCE: CORRESPONDENT BANKING SERVICES

FATF Recommendations

Recommendation 13. Correspondent banking

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

b) assess the respondent institution's AML/CFT controls;

c) obtain approval from senior management before establishing new correspondent relationships;

d) clearly understand the respective responsibilities of each institution; and

e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks.[87] Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

Interpretive Note to Recommendation 10 (Customer Due Diligence)

Higher Risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

b) Country or geographic risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

c) Product, service, transaction or delivery channel risk factors

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions where appropriate risk mitigation measures have not been implemented.
- Payment received from unknown or un-associated third parties.

Interpretive Note to Recommendation 10 (Customer Due Diligence)

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

D. ONGOING MONITORING AND REQUEST FOR INFORMATION ABOUT TRANSACTIONS

32. Where the monitoring system of the correspondent institution flags a transaction which could signal unusual activity, the correspondent institution should have internal processes to further review the activity, which may involve requesting transaction information of the respondent institution in order to clarify the situation and possibly clear the alert. This request for additional information should be targeted on the specific transaction which created an alert in the system, and could include, depending on the risk level of the transaction, a request to access information about the customer of the respondent institution as a means to get a proper understanding of the reasonableness of the transaction. This does not amount to a requirement to conduct CDD on the customer of the respondent. In practice, the correspondent institution will follow up with the respondent institution after the transaction is completed by making a request for information on that particular transaction(s) (RFI). Subsequently, the correspondent institution should also review its control systems in order to detect similar transactions. Such questions may include some, but not necessarily all, of the following:

- Duration of customer "X" relationship with the respondent institution and whether the respondent institution classifies the customer as a high risk customer.
- Purpose of the account(s) maintained by customer "X" (business, personal, other).
- Details of customer's "X" parent company and the name(s) of the beneficial owner(s).
- Source of the funds of customer "X".
- Consistency between the transactional history in the account profile of customer "X", and his KYC data, or with any other information available to the bank.
- Rationale of the transaction between customers "X" and a counterparty.
- Nature of the relationship between customers "X" and a counterparty.
- Possible affiliation of customers "X" with a third-party. Additional details regarding the goods/services being exchanged by the customers "X"and third-parties that are not found directly in the payment details of the transaction that may explain it.
- If possible, location of customer or third-party as originator/beneficiary and/or, n Status of the bank account of customer "X" (opened/closed).

33. Where the correspondent institution requests further information on a transaction from the respondent, it expects the respondent to respond in a timely fashion and provide documents/information to the level of detail requested. Where that does not happen, it may trigger concerns that the respondent is unable to manage its risks and lead to the filing of a suspicious transaction report by the correspondent institution. A request for information could be followed by a reassessment of the respondent's business and risk profile where/when necessary.

Endnotes

1. UNODC. https://www.unodc.org/unodc/en/money-laundering/overview.html
2. Bank for International Settlements, “Project Agorá: A shared programmable platform for wholesale cross-border payments”, p.7, 27 May 2026. https://www.bis.org/publ/othp110.pdf
3. RFI, “Congo Hold-Up: la BGFI, au cœur du scandale, brise le silence”, 25 November 2021. https://www.rfi.fr/fr/afrique/20211125-congo-hold-up-la-bgfi-au-c%C5%93ur-du-scandale-brise-le-silence
4. Gabonreview, “Congo Hold-Up’’ : Le Groupe BGFIBank réagit”, 24 November 2021. https://www.gabonreview.com/congo-hold-up-le-groupe-bgfibank-reagit/
5. Sonia Rolley (RFI) with Mediapart, “Congo Hold-Up: Sud Oil, la siphonneuse du premier cercle de Joseph Kabila”, 19 November 2021. https://www.rfi.fr/fr/afrique/20211119-congo-hold-up-sud-oil-la-siphonneuse-du-premier-cercle-de-joseph-kabila
6. The Sentry, “The Backchannel: State Capture and Bribery in Congo’s Deal of the Century”, pp. 13, 21 and 30, November 2021. https://thesentry.org/wp-content/uploads/2021/11/TheBackchannel-TheSentry-Nov2021.pdf; see also Sonia Rolley (RFI), “Congo Hold-Up: Congo Futur, un empire sous sanctions”, 26 November 2021. https://www.rfi.fr/fr/afrique/20211126-congo-hold-up-congo-futur-un-empire-sous-sanctions; and Sonia Rolley (RFI), “Congo Hold-Up: Congo Construction Company, le scandale du siècle”, 28 November 2021. https://www.rfi.fr/fr/afrique/20211128-congo-hold-up-congo-construction-company-le-scandale-du-si%C3%A8cle
7. RFI, “Congo Hold-Up: la BGFI, au cœur du scandale, brise le silence”, 25 November 2021. https://www.rfi.fr/fr/afrique/20211125-congo-hold-up-la-bgfi-au-c%C5%93ur-du-scandale-brise-le-silence
8. Aaron Krolik (The New York Times), “How a Small Chinese Bank Gave Moscow Access to Wall St.”, 9 October 2026. https://www.nytimes.com/2026/10/09/business/correspondent-banking-russia-sanctions-evasion.html
9. Aaron Krolik (The New York Times), “How a Small Chinese Bank Gave Moscow Access to Wall St.”, 9 October 2026. https://www.nytimes.com/2026/10/09/business/correspondent-banking-russia-sanctions-evasion.html
10. AFP (published by Actualite.cd), “‘Congo Hold-Up’ : une enquête préliminaire pour blanchiment ouverte en France”, 9 June 2022, https://actualite.cd/index.php/2022/06/09/congo-hold-une-enquete-preliminaire-pour-blanchiment-ouverte-en-france
11. Bank for International Settlements, Consultative Report: Correspondent Banking, p.7-8, 6 October 2015. http://www.bis.org/cpmi/publ/d136.pdf
12. European Central Bank, "Glossary of terms related to payment, clearing and settlement systems", 24 September 2024. https://www.ecb.europa.eu/services/glossary/html/act7a.en.html
13. IMF, “Staff Discussion Note : The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action”, p.11, June 2016. https://www.imf.org/external/pubs/ft/sdn/2016/sdn1606.pdf
14. Bank for International Settlements, “CPMI correspondent banking chartpack”, p.10 (Graph 8), May 2023. https://www.bis.org/pages/statistics/chartpack-2305.pdf
15. Tara Rice et al (Bank for International Settlements), “On the global retreat of correspondent banks”, 1 March 2020. https://www.bis.org/publications/global-retreat-correspondent-banks
16. FATF, “FATF Guidance: Correspondent Banking Services”, p.4, October 2015. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Correspondent-Banking-Services.pdf
17. Aaron Krolik (The New York Times), “How a Small Chinese Bank Gave Moscow Access to Wall St.”, 9 October 2026. https://www.nytimes.com/2026/10/09/business/correspondent-banking-russia-sanctions-evasion.html
18. FATF, “FATF clarifies risk-based approach: case-by-case, not wholesale de-risking”, 23 October 2014. https://www.fatf-gafi.org/en/publications/fatfgeneral/documents/rba-and-de-risking.html
19. Egbuna, Ngozi Eunice et al. (Institut Monétaire de l'Afrique de l'Ouest (IMAO), Accra), Série de publications occasionnelles de l’IMAO, No. 25), “Déclin des relations de correspondance bancaire dans la Zone Monétaire de l'Afrique de l'Ouest”, p.5-6, December 2021. https://www.econstor.eu/bitstream/10419/270758/1/OPS25fre.pdf
20. BCBS, “Guidelines: Revised annex on correspondent banking – Consultative Document”, 23 November 2016. https://www.bis.org/bcbs/publ/d389.pdf
21. The Wolfsberg Group, Wolfsberg Financial Crime Principles for Correspondent Banking, 28 October 2022. https://db.wolfsberg-group.org/assets/d39a5072-7fb6-4e31-9a87-9e54021ce71f/Wolfsberg%20Correspondent%20Banking%20Principles%202022.pdf
22. US Department of the Treasury and Federal Banking Agencies, “Joint Fact Sheet on Foreign Correspondent Banking: Approach to BSA/AML and OFAC Sanctions Supervision and Enforcement”, 30 August 2016. https://comptrollerofthecurrency.gov/publications-and-resources/publications/banker-education/files/pub-foreign-correspondent-banking-fact-sheet.pdf; see also Aaron Krolik (The New York Times), “How a Small Chinese Bank Gave Moscow Access to Wall St.”, 9 October 2026. https://www.nytimes.com/2026/10/09/business/correspondent-banking-russia-sanctions-evasion.html
23. Bank for International Settlements, “CPMI correspondent banking chartpack”, p.10 (Graph 3), May 2023. https://www.bis.org/pages/statistics/chartpack-2305.pdf

24. United States Code, International Emergency Economic Powers Act (50 U.S.C. ch. 35, §§ 1701–1710). https://www.law.cornell.edu/uscode/text/50/chapter-35
25. United States Code, Trading with the Enemy Act (50 U.S.C. ch. 53, §§ 4301–4341). https://www.law.cornell.edu/uscode/text/50/chapter-53
26. DOJ, "BNP Paribas Agrees to Plead Guilty and to Pay $8.9 Billion for Illegally Processing Financial Transactions for Countries Subject to US Economic Sanctions", 30 June 2014. https://www.justice.gov/archives/opa/pr/bnp-paribas-agrees-plead-guilty-and-pay-89-billion-illegally-processing-financial
27. DOJ, "Standard Chartered Bank Admits to Illegally Processing Transactions in Violation of Iranian Sanctions and Agrees to Pay More Than $1 Billion", 9 April 2019. https://www.justice.gov/archives/opa/pr/standard-chartered-bank-admits-illegally-processing-transactions-violation-iranian-sanctions; see also Financial Conduct Authority, "FCA fines Standard Chartered Bank £102.2 million for poor AML controls", 9 April 2019. https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls
28. United States Code, Bank Secrecy Act (12 U.S.C. §§ 1829b, 1951–1960; 31 U.S.C. §§ 5311–5314, 5316–5336). https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act
29. DOJ, "HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement", 11 December 2012. https://www.justice.gov/archives/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations
30. DOJ, "United States v. Commerzbank AG and Commerzbank AG New York Branch: Deferred Prosecution Agreement" (No. 15-00031, D.D.C.), 12 March 2015. https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf
31. Aaron Krolik (The New York Times), "How a Small Chinese Bank Gave Moscow Access to Wall St.", 9 October 2026. https://www.nytimes.com/2026/10/09/business/correspondent-banking-russia-sanctions-evasion.html
32. AMLA, "About AMLA". https://www.amla.europa.eu/about-amla_en
33. DOJ, "Press Release: Danske Bank pleads guilty to fraud on US banks in multi-billion dollar scheme to access the US Financial System", 13 December 2022. https://www.justice.gov/opa/pr/danske-bank-pleads-guilty-fraud-us-banks-multi-billion-dollar-scheme-access-us-financial
34. OCCRP, "'The Contract Factory': Inside Danske Bank Estonia's Money Laundering Machine", 23 February 2022. https://www.occrp.org/en/project/the-azerbaijani-laundromat/the-contract-factory-inside-danske-bank-estonias-money-laundering-machine
35. The Guardian, "Whistleblower at Danske Bank Was Firm's Baltics Trading Head", 26 September 2018. https://www.theguardian.com/world/2018/sep/26/danske-bank-whistleblower-was-ex-baltics-trading-head-howard-wilkinson
36. The Guardian, "Whistleblower reveals more players in £178bn Danske Bank scandal", 19 November 2018. https://www.theguardian.com/business/2018/nov/19/whistleblower-reveals-more-players-in-178bn-danske-bank-scandal
37. Reuters, "U.S. investigators approach Deutsche Bank, BofA, JPM in Danske probe: Bloomberg", 16 November 2018. https://www.reuters.com/article/business/us-investigators-approach-deutsche-bank-bofa-jpm-in-danske-probe-bloomberg-idUSKCN1NL1HD/
38. OCCRP, "Deutsche Bank Investigated for Role in Danske Scandal", February 2019. https://www.occrp.org/en/news/deutsche-bank-investigated-for-role-in-danske-scandal
39. ACAMS, "Fed Fines Deutsche Bank $186 Million for Failure to Address AML Issues", 19 July 2023. https://www.acams.org/en/news/fed-fines-deutsche-bank-186-million-for-failure-to-address-aml-issues
40. NYDFS, "Superintendent Adrienne A. Harris Secures $35 Million Settlement", 27 August 2024. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20240827
41. Nordea, "Inside information: Nordea receives verdict in case about anti-money laundering measures from 2012 to 2015", 9 November 2026. https://www.nordea.com/en/press/2026-11-09/inside-information-nordea-receives-verdict-in-case-about-anti-money-laundering-measures-from-2012-to-2015
42. AML Intelligence, "FIMbank hit with €168,942 fine over failings in AML regime", August 2020. https://www.amlintelligence.com/2020/08/fimbank-hit-with-e168942-fine-over-failings-in-aml-regime/
43. Mediapart, "La justice française ouvre une enquête après les révélations de Congo Hold-up", 8 June 2022. https://www.mediapart.fr/journal/international/080622/la-justice-francaise-ouvre-une-enquete-apres-les-revelations-de-congo-hold
44. Aaron Krolik (The New York Times), "How a Small Chinese Bank Gave Moscow Access to Wall St.", 9 October 2026. https://www.nytimes.com/2026/10/09/business/correspondent-banking-russia-sanctions-evasion.html
45. Groupe d'Action contre le Blanchiment d'Argent en Afrique Centrale (GABAC), "Anti-Money Laundering and Counter-Terrorist Financing Measures: Democratic Republic of Congo, Mutual Evaluation Report", 2021. https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-mer/GABAC-MER-DRC-2021.pdf.coredownload.inline.pdf
46. Sonia Rolley (RFI), "Congo Hold-Up: Congo Futur, un empire sous sanctions", 26 November 2021, https://www.rfi.fr/fr/afrique/20211126-congo-hold-up-congo-futur-un-empire-sous-sanctions

47. Sonia Rolley (RFI), “Congo Hold-Up: Congo Futur, un empire sous sanctions”, RFI, 26 November 2021, https://www.rfi.fr/fr/afrique/20211126-congo-hold-up-congo-futur-un-empire-sous-sanctions; see also, Nada Maucourant Atallah (L’Orient Today), “How did the network of Tajeddine companies circumvent US sanctions against Hezbollah?”, 24 November 2021. https://today.lorientlejour.com/article/1282561/how-did-the-network-of-tajeddine-companies-circumvent-us-sanctions-against-hezbollah.html
48. The Sentry, “The Backchannel: State Capture and Bribery in Congo’s Deal of the Century”, November 2021. https://thesentry.org/wp-content/uploads/2021/11/TheBackchannel-TheSentry-Nov2021.pdf
49. The Sentry, “The Backchannel: State Capture and Bribery in Congo’s Deal of the Century”, November 2021. https://thesentry.org/wp-content/uploads/2021/11/TheBackchannel-TheSentry-Nov2021.pdf
50. IMF, “Global Cross-Border Payments: A $1 Quadrillion Evolving Market?”, June 2025, p. 5. https://www.imf.org/-/media/files/publications/wp/2025/english/wpiea2025120-print-pdf.pdf (“Swift represents the primary communication channel for financial institutions, market infrastructures, corporates, and central banks to transmit messages related to international financial payments, securities, foreign exchange transactions, treasury operations, and trade finance. Messages transmitted via the Swift network must adhere to standardised codes to ensure that practices and conventions align effectively across users”)
51. The Sentry, “The Backchannel: State Capture and Bribery in Congo’s Deal of the Century”, p.20, November 2021. https://thesentry.org/wp-content/uploads/2021/11/TheBackchannel-TheSentry-Nov2021.pdf
52. Sonia Rolley (RFI), “Congo Hold-Up: Congo Construction Company, le scandale du siècle”, 28 November 2021, https://www.rfi.fr/fr/afrique/20211128-congo-hold-up-congo-construction-company-le-scandale-du-si%C3%A8cle;
53. La Libre Belgique, “RDC : une information judiciaire ouverte contre le clan Kabila”, 25 November 2021. https://www.lalibre.be/international/afrique/2021/11/25/rdc-une-information-judiciaire-ouverte-contre-le-clan-kabila-6Q6G2PQEHBDKZKNGQ7Z453LC4Y/
54. William Clowes and Michael Kavanagh, “China built Congo a toll road that led straight to the ruling family”, Bloomberg News, republished by MINING.COM, 3 February 2022. https://www.mining.com/web/china-built-congo-a-toll-road-that-led-straight-to-the-ruling-family/
55. Banco de España, “The Banco de España fines Depasify”, 29 April 2025. https://www.publicnow.com/view/216A3CC811DC136540347CF99229E7F1C7D7D112?1745945129
56. Sonia Rolley (RFI) and Yann Philippin (Mediapart), “Congo Hold-Up: Egal, l’autopsie d’un scandale”, RFI, 22 November 2021 (updated 23 November 2021). https://www.rfi.fr/fr/afrique/20211122-congo-hold-up-egal-l-autopsie-d-un-scandale
57. Sonia Rolley and Christina Okello (RFI), “Congo Hold-Up: on the trail of Joseph Kabila's mystery company”, 5 December 2021. https://www.rfi.fr/en/africa/20211205-congo-hold-up-on-the-trail-of-joseph-kabila-s-mystery-company-port-de-fisher-corruption-tax-haven-bank
58. Xavier Monnier (Le Monde Afrique), “Au Cap, le mystérieux yacht de luxe des partenaires d’affaires du président Kabila”, 11 July 2017. https://www.lemonde.fr/afrique/article/2017/07/11/le-mysterieux-yacht-de-luxe-des-partenaires-d-affaires-du-president-kabila_5159113_3212.html
59. Sonia Rolley (RFI), “Congo Hold-Up: Congo Construction Company, le scandale du siècle”, RFI, 28 November 2021, https://www.rfi.fr/fr/afrique/20211128-congo-hold-up-congo-construction-company-le-scandale-du-si%C3%A8cle
60. Sonia Rolley (RFI) and Yann Philippin (Mediapart), “Congo Hold-Up: Egal, l’autopsie d’un scandale”, 22 November 2021 (updated 23 November 2021). https://www.rfi.fr/fr/afrique/20211122-congo-hold-up-egal-l-autopsie-d-un-scandale
61. Gabonreview, “Congo Hold-Up’’ : Le Groupe BGFIBank réagit”, 24 November 2021. https://www.gabonreview.com/congo-hold-up-le-groupe-bgfibank-reagit/
62. FATF, “FATF Guidance: Correspondent Banking Services”, p.15-16, October 2015. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Correspondent-Banking-Services.pdf
63. Africa Confidential, “Exposed – the cost of Kabila’s state capture”, 19 November 2021. https://www.africa-confidential.com/article/id/13683/exposed-%e2%80%93-the-cost-of-kabilas-state-capture%c2%a0
64. Sonia Rolley (RFI) with Mediapart, “Congo Hold-Up: Sud Oil, la siphonneuse du premier cercle de Joseph Kabila”, 19 November 2021. https://www.rfi.fr/fr/afrique/20211119-congo-hold-up-sud-oil-la-siphonneuse-du-premier-cercle-de-joseph-kabila, see also The Sentry, “The Backchannel: State Capture and Bribery in Congo’s Deal of the Century”, p.11, November 2021. https://thesentry.org/wp-content/uploads/2021/11/TheBackchannel-TheSentry-Nov2021.pdf
65. La Libre Belgique, “RDC : une information judiciaire ouverte contre le clan Kabila”, 25 November 2021. https://www.lalibre.be/international/afrique/2021/11/25/rdc-une-information-judiciaire-ouverte-contre-le-clan-kabila-6Q6G2PQEHBDKZKNGQ7Z453LC4Y/
66. Sonia Rolley (RFI), “Congo Hold-Up: Congo Construction Company, le scandale du siècle”, 28 November 2021. https://www.rfi.fr/fr/afrique/20211128-congo-hold-up-congo-construction-company-le-scandale-du-si%C3%A8cle; see also The Sentry, “The Backchannel: State Capture and Bribery in Congo’s Deal of the Century”, pp.9 and 11, November 2021. https://thesentry.org/wp-content/uploads/2021/11/TheBackchannel-TheSentry-Nov2021.pdf

67. PPLAAF, “Democratic Republic of Congo: Major Road Project Built on Corruption Risk”, 18 July 2025. https://www.pplaaf.org/2025/07/18/democratic-republic-of-congo-major-road-project-built-on-corruption-risk.html
68. Bloomberg, “China built Congo a toll road that led straight to the ruling family”, 3 February 2022. https://www.bloomberg.com/news/features/2022-02-03/congo-s-kabila-family-made-millions-off-toll-road-built-by-china
69. Vitruvius Yachts, “The Refitted 71m Superyacht – Enigma XK”. https://vitruviusyachts.com/our-world/the-refitted-71m-superyacht/
70. RFI, “Congo Hold-Up: on the trail of Joseph Kabila’s mystery company”, 5 December 2021. https://www.rfi.fr/en/africa/20211205-congo-hold-up-on-the-trail-of-joseph-kabila-s-mystery-company-port-de-fisher-corruption-tax-haven-bank
71. Sonia Rolley (RFI), “Congo Hold-Up: comment transférer des millions à l’étranger?”, 27 November 2021. https://www.rfi.fr/fr/afrique/20211127-congo-hold-up-comment-transf%C3%A9rer-des-millions-%C3%A0-l-%C3%A9tranger
72. FATF, “The Role of Hawala and Other Similar Service Providers in ML/TF”, October 2013. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Role-hawalas-in-ml-tf.html
73. PPLAAF, “The Lumumba Papers”. https://www.pplaaf.org/cases/the-lumumba-papers.html; see also RFI, “Congo Hold-Up: trois millions de dollars d'argent public retirés en cash par le directeur financier de Kabila”, 30 November 2021. https://www.rfi.fr/fr/afrique/20211130-congo-hold-up-trois-millions-de-dollars-d-argent-public-retir%C3%A9s-en-cash-par-le-directeur-financier-de-kabila
74. Sonia Rolley (RFI) and Yann Philippin (Mediapart), “Congo Hold-Up: Egal, l’autopsie d’un scandale”, 22 November 2021 (updated 23 November 2021). https://www.rfi.fr/fr/afrique/20211122-congo-hold-up-egal-l-autopsie-d-un-scandale
75. Khadija Sharife (OCCRP), “DRC Company Promised Cheap Food, Delivers Stolen Money”, 8 November 2017. https://www.occrp.org/en/investigation/drc-company-promised-cheap-food-delivers-stolen-money
76. The Sentry, “The Backchannel: State Capture and Bribery in Congo’s Deal of the Century”, p.20-21 and Annex 2, November 2021. https://thesentry.org/wp-content/uploads/2021/11/TheBackchannel-TheSentry-Nov2021.pdf
77. DOJ, “Commerzbank AG Admits to Sanctions and Bank Secrecy Violations, Agrees to Forfeit $563 Million and Pay $79 Million Fine”, 12 March 2015. https://www.justice.gov/usao-dc/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million
78. Commerzbank, “Annual Report 2016”, p.53, 23 March 2017. https://investor-relations.commerzbank.com/media/document/032db93a-9363-4c9a-9031-4b9d23e2b574/assets/Geschaeftsbericht_2016_Konzern_EN.pdf?disposition=inline
79. Aaron Krolik (The New York Times), “How a Small Chinese Bank Gave Moscow Access to Wall St.”, 9 October 2026. https://www.nytimes.com/2026/10/09/business/correspondent-banking-russia-sanctions-evasion.html


ANTI
CORRUPTION
DATA COLLECTIVE


PPLAAF