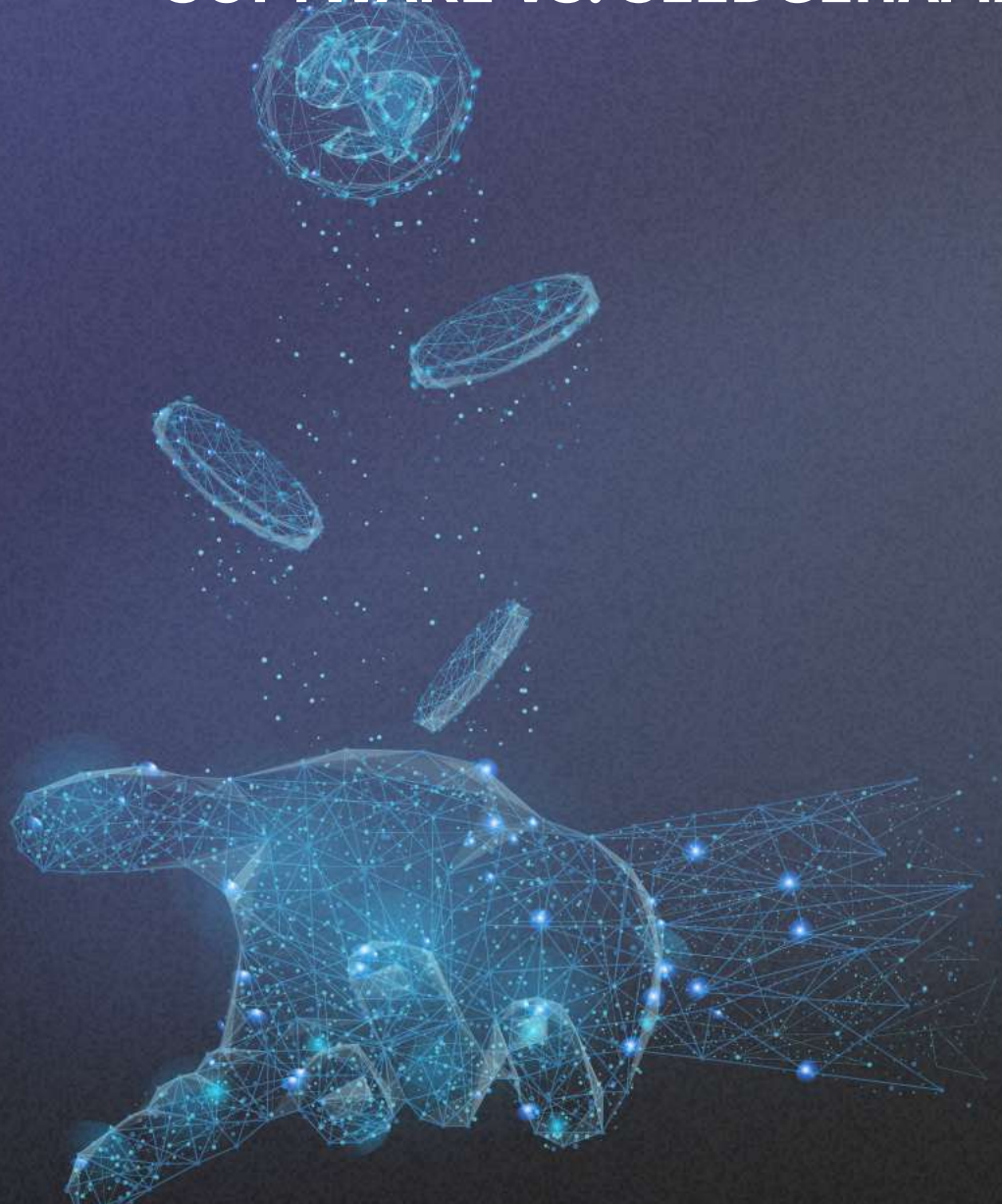


DE-RISKING CROSS-BORDER PAYMENTS: SOFTWARE VS. SLEDGEHAMMER



MARCH 2024

de-risking :

Overview

De-risking refers to the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk.

<https://www.state.gov/de-risking/> :

FOREWORD

Reimagining Correspondent Banking for Cross-Border Payments: The ‘Way We’ve Always Done It Doesn’t Work’

It’s mind-blowing (and quite scary) that after 50 years, financial institutions and others in the cross-border ecosystem are executing millions of manual processes each day at originating institutions, intermediate and correspondent banks to process an international money transfer.

Why is this so scary? Because our **global economy is 100% dependent on these expensive, slow and error-prone manual processes**, including dysfunctional data and document collection, spotty validation and minimal visibility or sharing among others in the ecosystem to complete payments.

And we wonder why cross-border payments are high-risk, slow and expensive.

I’ve decided to depart from convention and approach this foreword in an unorthodox manner by asking questions that expose the depth and breadth of the problem.

Questions for originating institutions

1. When an FI customer presses “submit” on the bank’s website to make a cross-border payment, why do they learn later, sometimes days or weeks later, and perhaps only after calling the FI and asking “where’s my money?” that they are required to provide a bill of lading, invoice, customs declaration or other “evidence” to justify the payment?
2. When a bank’s customer inquires about “why” a payment was held, why can’t the question be answered? Or depending on who takes the call, the answers are different. Why is FinCEN blamed for stopping the payment? Why do many banks require the request in writing sent to wiretransferscompliance@nameyourbank.com? And why does it take days, or weeks for a reply—if one is ever provided?
3. Why aren’t bulk or mass cross-border payments to marketplace sellers, contractors, vendors, missionaries, class action claimants, employees or others easy? Or even possible? Why is one-by-one entry the norm.
4. Why can’t cross-border payments be integrated into a bank customer’s business processes with APIs or file transfers offered by the FI?
5. Why do only the largest FIs in a country make a profit from cross-border payments and others lose money?
6. Why are most FIs forced to “buy” this product from their competitors?
7. Why is the number of FIs that offer cross-border payments shrinking? Does this inspire fintechs and digital innovators to compete?
8. Why are dozens of risk, compliance and other policies and procedures manually executed?
9. Why are bank customers generally very unhappy with the international money transfer experience?
10. Why does it take so long for a cross-border payment to arrive—especially when funds are actually “in-country” with the correspondent bank, so liquidity is not the issue?

Questions for correspondent, intermediate and domestic clearing banks

11. Why are correspondent banks or intermediate banks needed at all?

12. Why doesn't the intermediate bank or correspondent bank delivering the payment to a recipient have "see-through" to data, document and artifact rich KYC and KYT details?

13. Before **every** cross-border transaction is delivered, why isn't there a systemic authorization routine that considers the disburser's KYC, their commercial activity or source of funds, the eIDV and sanctions checks of owners/officers/directors and the documentary evidence substantiating the legitimacy of the payment?

14. If "see-through" was magically possible on 100% of all transactions, why, under specific risk or other conditions, can't a correspondent or intermediate bank execute digital consent to permit direct execution of "Know Your Customer's Customer" and independently and systemically verify eIDV, sanctions checks and other risk or compliance routine versus "trusting" the originating institution?

15. Why are Know Your Transaction audits defined as an after-the-fact (up to two years!) painstaking and manual look-back versus a real-time event on 100% of transactions where data and artifacts are interrogated as part of an authorization routine?

16. Why do correspondent banks require massive

nostro-vostro account balances and expose foreign partner FIs to P&L risks and balance sheet complications from currency volatility?

17. Why are midsize and smaller FIs constantly "de-risked" from this lucrative business and volumes concentrated with fewer and fewer of the massive FIs? Let me be provocative—it's true larger FIs can afford to pay bigger fines when they're eventually tagged, but is this good for anyone? And rarely are their fraud and risk mitigation procedures or capabilities any better than midsize or smaller FIs—although they can afford to throw "more humans" at any problem.

18. Why are the due diligence checklists or documentation requirements for foreign FIs, MSBs, EMLs, PIs and other regulated entities reflected in Excel spreadsheets that are often out-of-date?

19. Why are there mountains of paper or shared files or other poorly organized and stored data, leading to incomplete, or entirely missing audit trails?

20. When a payment instruction is received from a foreign FI, why are these manually keyed into a core bank or other system by the majority of correspondent, intermediate or clearing banks?

21. Why is it so difficult, slow and costly to administer nostro-vostro, FBO, ring-fenced and other fiduciary accounts?

Questions for central banks, regulators and payment networks

22. What would give regulators confidence to allow, if not encourage, versus discourage more competition among correspondent, intermediate and clearing banks?

23. Why are examinations of financial institutions in the cross-border ecosystem so long, labor intensive and dependent on slow and extensive research?

24. Why can't they see and/or systemically interrogate, or at least view payer and recipient documentary details, and under rules- or risk-based conditions pause a transaction for inspection on every in-bound or out-bound cross-border payment in real-time?

25. What's the root cause of FIs failing so often to execute their own risk, compliance and operating procedures as originators and clearing or correspondent banks and how can this be fixed?

26. And are the stated goals of central banks and regulators to foster safe, efficient (fast and low cost), transparent and inclusive cross-border payments even possible with the current correspondent banking construct and typical core banking, digital banking and compliance systems?

In an age where digital transformation has touched every industry, financial institutions around the world are sending and receiving money internationally the old-fashioned way—if they are willing (or allowed) to take the “risk” at all.

For the shrinking number of banks, credit unions and building societies that offer or clear cross-border payments, the questions above provide clear and specific insight into why these payments are slow, expensive, opaque and frustrating for their customers.

In this whitepaper, author Jonathan Tyce explores the regulatory environment, as well as the operational and market realities squeezing U.S. based correspondent banks that clear foreign-initiated payments. But many of his takeaways apply to any bank around the world supporting foreign banks with their cross-border payments needs. And he questions the age-old, hammer-like act of “de-risking”.

The Bottom Line

Purpose-built software or proper digital infrastructure for the cross-border ecosystem IS the solution. From directly addressing what have been intractable problems, to enabling smarter and more effective rules as well as new paradigms by regulatory bodies—technological breakthroughs convincingly overcome the root causes of the issues.

It's not easy, but it's doable. It's not that expensive, and the ROI is compelling. And the time is now—not in some far-off future.

Don't limit your thinking to “how things have always been done,” or assume the problem is too big to solve.

Gary

President and CEO

Payall Payment Systems

P.S. I asked 26 questions; I have another 20 or 30 common-sense, basic questions—too many to ask here.

If you'd like to read them all, drop me an email at gary.palmer@payallps.com and I'll send them.

CONTENTS

De-Risking Cross-Border Payments: Software vs. Sledgehammer

Foreword	I
A Few Words from Jerome Powell	05
Introduction	06
3 Observations, 2 Predictions, 1 Suggestion	09
3 Observations	09
A Window of Opportunity Is Closing	
The Majority of Violations Have an Easy Fix	
Trust Between Regulators & Banks Can Easily Be Improved	
2 Predictions	14
Software Will Cut Costs by 50%, Violations by 90%	
End-to-End Visibility Becomes Available to Regulators	
1 Suggestion	16
FinCEN Can Ease Tensions by Sharing More Information	
Crossed Wires: Why Does De-Risking Happen?	17
Automating Trust & the Birth of See-Through	20
Software Is a Neutral Player	22



“There’s a way to do it better. Find it.”

THOMAS EDISON

‘Trust’ Between Regulators & Banks Can Easily Be Improved

A FEW WORDS FROM JEROME POWELL

“

“The goal of the FSB roadmap is simple—to create an ecosystem for cross-border payments that is faster, cheaper, more transparent, and more inclusive.”



Source: *NY Magazine*, 2020. <https://nymag.com/intelligencer/article/jerome-powell-federal-reserve-profile.html>

“As the roadmap makes clear, one of the keys to moving forward will be doing both—improving the existing system where we can while also evaluating the potential of and the best uses for emerging technologies.

“Improvements in the global payments system will come not just from the public sector, but from the private sector as well,” Powell continued. “[T]he private sector has the experience and expertise to develop consumer-facing infrastructure that improves and simplifies how the public engages with the financial system.”

“Digitalization of financial services, combined with an improved consumer experience, can help increase financial inclusion, particularly in countries or areas with a large unbanked population...

“... it is only by engaging all stakeholders—policymakers, private-sector participants, and academia—as this conference is doing, that we will achieve the improved payments ecosystem we are striving toward.”

Committee on Payments
and Market Infrastructures



Source: Presented at “Pushing the Frontiers of Payments: Towards Faster, Cheaper, More Transparent and More Inclusive Cross-Border Payments” Conference, Committee on Payments and Market Infrastructures, Basel, Switzerland, March 2021

Powell’s comments were made in early 2021. The frenzy following Covid-19 lockdowns and the anticipated acceleration of the shift to a digital world had driven PayPal’s market capitalization to beyond \$300 billion, versus less than \$70 billion currently. While PayPal has not been able to maintain its high market cap, Powell’s observations about what it will take to improve cross-border payments still ring true.

However, the capacity of the private sector and technology is not simply limited to the consumer-facing experience. Digital verification, data storage and assimilation, time and cost efficiencies, and the automation of trust are also what private sector software and technology can add to the mix.

INTRODUCTION

The U.S. is not alone in grappling with the convoluted and unintended consequences of de-risking, but its struggle looks set to become more complex this year and next thanks to an unprecedented confluence of factors. How to deliver real transparency and achieve true “see-through” as well as optionally, KYCC (know your customer’s customer) are concepts that are re-defined and the bedrock of this paper, as the fight to stem the flow of laundered money globally—estimated at between \$2 trillion and \$4 trillion annually—continues.

This paper will make three observations about the state of play in cross-border payments (foreign-initiated into the U.S.), volunteer two bold predictions and posit one suggestion about the most effective place to start.

The motivations behind regulatory de-risking are intended to be fundamentally positive, as the U.S.’s Financial Action Task Force was at pains to reiterate as far back as October 2014.



“

“De-risking’ should never be an excuse for a bank to avoid implementing a risk-based approach, in line with the FATF standards. The FATF Recommendations only require financial institutions to **terminate customer relationships, on a case-by-case basis, where the money laundering and terrorist financing risks cannot be mitigated.**”

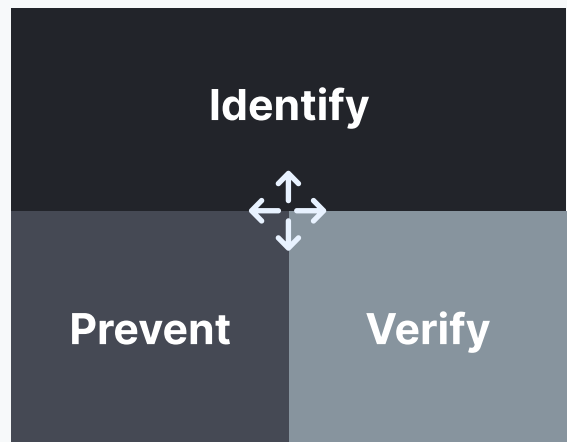
FINANCIAL ACTION TASK FORCE,
OCTOBER 2014

But in reality, most U.S. banks terminate a larger number, if not all of financial institution and other customer relationships as an immediate reaction to an FATF notice of an Increased Monitoring or gray-list designation of a jurisdiction.

As a result, the unintended consequences of de-risking continue to spill over, and the roster of victims—poorer nations, lower income citizens and non-profit organizations to name but a few—is growing.

Regulators from Australia to the European Union, India to Sweden, are jointly embroiled in this long-term endeavor but, as this paper will explore, the U.S. faces a unique cocktail of pressures and often conflicting forces.

At its heart, three words encapsulate the challenge—**Identify, Verify** and **Prevent**.



Did You Know?

In 92% of the world's countries and territories, three or more FIs made cross-border payments on the Swift network in 1Q23.

Don't Close The Stable Door After the Horse Has Bolted



"Just a minute!"

De-risking is extensively analyzed, so this paper will attempt to avoid the well-trodden path. The phenomenon has worsened considerably in recent years. Debate is too often skewed toward intangible or high-level obstacles and the risk-based vagaries of the problem and too seldom on practical solutions. Ironically, and in keeping with the centuries-old proverb about closing the stable door after the horse has bolted, this could exacerbate what is already a stiff challenge.

TWO UNDER-APPRECIATED UNINTENDED CONSEQUENCES OF DE-RISKING

- De-risking banks often doesn't actually de-risk the U.S. payments system—it just shifts the business;
- De-risking the system lowers competition and the competitive pressure to innovate, invest and improve efficiencies.

THE GOALS OF THIS PAPER ARE TO

- Reorder the ranking and narrative on the causes of many of the problems with de-risking;
- Propose steps toward best practices that can alleviate and/or reverse the need for de-risking;

- Encourage collaboration through action to bolster public and private sector investment, improve trust and transparency, and lower frictions.

Technology to the Rescue?

A key focus that belongs near the top of the actionable agenda is technology. Surprisingly, this topic is not even explored until deep (page 48) into the Department of Treasury's 54-page, April 2023 De-risking Strategy paper.

"Automation" is not mentioned once in the AMLA paper, "technology" only 3 times; "digital" a paltry 10 times, versus 51 uses of "risk-based" and 110 "AML/CFTs".

AMLA

The Department of the Treasury's
De-risking Strategy



ADVERSE CONSEQUENCES OF DE-RISKING

- Increased use of unregulated financial channels
- Curtailment of financial access
- Development funding and humanitarian and disaster relief
- Correspondent consolidation
- Geopolitical concerns

h. Explore the Potential for Emerging Technological Solutions, Including Digital Identity

"Digital identity solutions could also potentially address de-risking by increasing the efficiency and safety of customer identification data storage and processes that banks and MSBs."

Source: AMLA: https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf



“The advance of technology is based on making it fit in so that you don’t even really notice it, so it’s part of everyday life.”

BILL GATES

THIS PAPER WILL SHOW:

- The right technologies are not emerging, they are already here, and still faster and better solutions are around the corner.
- Digital is under-represented in this debate and must be pushed far higher up the agenda to keep pace with what is and will become possible.
- Software and automation can already address and resolve many aspects of the de-risking conundrum.

As the reality of real-time payments spreads globally, the role that software must play has to be recognized and encouraged. Regulators talk about regulation because that is what regulators do. Regulators and enforcement agencies can also drive, encourage and steer investment, collaboration and progress and that is what they should also strive to do.

3, 2, 1: Smoothing Tensions with Neutral Players

The next chapter will posit 3 observations, 2 predictions and 1 suggestion for U.S. stakeholders about de-risking and the cross-border payments industry, with a specific focus on foreign-initiated payments to the U.S. The key takeaways and issues will be fleshed out in the *Crossed Wires: Why Does De-Risking Happen?* section.

How automation and technology has already changed the game will be detailed in *Automating Trust & the Birth of See-Through*, as each critical step of the KYCC process (know your customer’s customer) is examined.

Software Is a Neutral Player will show how technology can smooth many of the tensions between regulators and the regulated, effectively killing two birds with one stone.

An Early Note of Caution

A degree of realism and caution is also warranted. Previous well-intentioned actions and regulations of those looking to prevent money laundering and financing of terrorism have also created a number of unintended consequences. So too, technological breakthroughs—while undeniably the path to resolving many problems—will also bring unintended consequences of their own.

This paper and the software and automation advances that it will discuss are just the start of the next phase of global cross-border payment development.



“Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks.”

STEPHEN HAWKING

Did You Know?

The global average cost of sending a \$200 USD remittance is 6.3%.

3 OBSERVATIONS, 2 PREDICTIONS, 1 SUGGESTION

3 OBSERVATIONS

A Window of Opportunity Is Closing

The need to address, resolve and reverse many of the problems of de-risking is becoming more pressing, with a confluence of drivers building a sense of urgency in 2024.

Successfully regulating the cross-border industry and payment flows into the U.S. will become yet more challenging as the market share of traditional, U.S.-based correspondent banks continues to fall.

Regulators can and should act now to encourage and collaborate with banks to invest in the right technology and solutions to mitigate risk, not exacerbate de-risking by an overarching focus on risk-based strictures or termination of relationships.

CROSS-BORDER PAYMENTS ARE FOR THE BANKS TO LOSE

Market Share Loss

De-Risking Cross-Border Payments:
Software vs. Sledgehammer
Jonathan Tyce interviewing Stan Cole

00:00 43:05

STAN COLE
Payments specialist, Advisor, UNITE GLOBAL AS

The classic correspondent banks' market share decline is set to accelerate given de-risking and as the likes of Mastercard and Visa continue to grow in new business lines. Non-regulated, digital innovators or other channels are also increasingly used. In the echelons of cross-border payments, the tech giants from Apple to Google to PayPal are also changing the game.

Further, the most obvious victims of the unintended consequences of de-risking—non-profit organizations, higher-risk countries, humanitarian aid and the unbanked or poor who are dependent on remittances to survive—will have their troubles compounded by heightened global geopolitical unrest, with elections, populism, war and the aftermath of a sea-change in inflation and interest rates feeding through the system in 2024.

“

“Fintech is nibbling the banks' lunch, but guess who is eating the banks' lunch more than Fintech! It's the giants—it's Visa and Mastercard.”

STAN COLE, PAYMENTS SPECIALIST,
EX-CORRESPONDENT BANKER

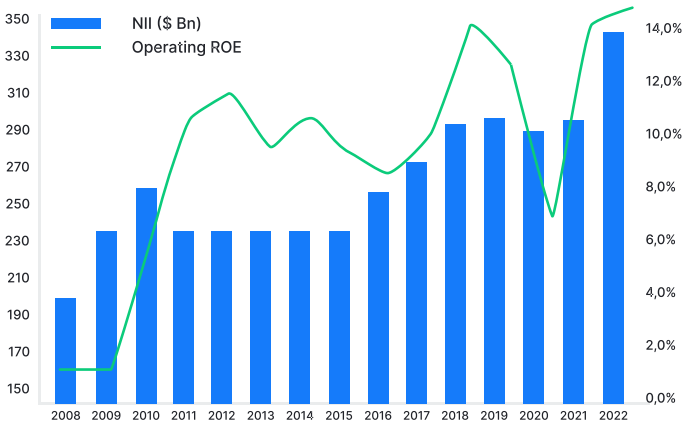
“

“My own theory is that we are in the middle of a dramatic and broad technological and economic shift in which software companies are poised to take over large swathes of the economy.”

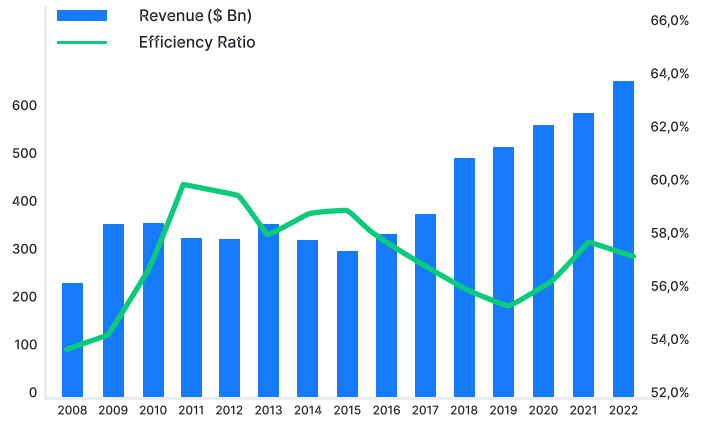
MARC ANDREESEN

PEAK PROFITABILITY IS THE TIME TO ACT: COLLABORATE & INVEST

U.S. Regional Banks: ROE vs. NII



U.S. Regional Banks: Efficiency Ratio vs. Revenue



Source: Bloomberg, 2018: <https://www.bloomberg.com/view/articles/2018-05-22/10-k-company-filings-are-actually-worth-reading>

For the U.S. regional banking sector, the midsize players that are the focal point of this paper, profitability is back to multi-year highs. As the tailwind of higher interest rates dies, likely within four quarters, the cyclical shift from interest income growth back to a focus on fees and cost control will take hold. Wall Street estimates imply that operating returns-on-equity for this sector will fall 1-2 percentage points over 2024-25 to about 12%.

Typically, software and equipment expenses for a midsize bank represent about 10% of non-interest expenses. Encouraging and incentivizing the banks to invest now will help lower future efficiency ratios to below 60%, slow the trajectory of non-performing assets and ease charge-off rates, as well as mitigate risk of fines. There are many ways to do this, and as the European Banking Authority clearly acknowledged in 2020, this goal should remain high on the global regulatory agenda.



“Considering the increasing relevance that software assets and technology in general are assuming in the financial and banking sector, it is important to encourage IT investments with the aim of supporting the technological development and modernisation of the sector, given its importance also from a competitive perspective.”

EUROPEAN BANKING AUTHORITY, OCTOBER 2020

The Majority of Violations Have an Easy Fix

In the majority of cases, the reasons behind correspondent banks' BSA violations are almost always shockingly simple. Human error, a lack of eyes on the data and low human capital investment are to blame. Occasionally, a bank turns a blind-eye—either through indolence or willfull neglect, in the most egregious examples.

The root cause is clear. Just as airlines trust and use software to land jumbo jets thousands of times daily, new software must be more widely employed in payments. Automation to improve the efficiency, proper execution and transparency of failed tasks that cause these BSA violations—software for all of this is now available. Historically, it's never been part of a bank's core systems or digital platform because it wasn't possible. It is now.


THREE REASONS EXAMINERS CALL FOR DE-RISKING

The most common reason that examiners de-risk banks from offering cross-border payments is that, when audited, they are found to have failed to follow their own policies, procedures and practices (the three P's) submitted to the regulators.

Why? Very often, it is because the procedures are manual and workers are fallible. If this is the case, a warning is usually issued to the bank, with a request to "do better." Very occasionally, the bank may be asked to cease offering cross-border payments immediately.

In some cases, a bank may face being de-risked despite following its own protocols. The problem here is fueled by the discovery that the initiating foreign institution failed to follow its own policies and procedures (again likely because it is a manual process). Where this failure involves AML checks or a sanctions list omission, the consequences can escalate rapidly.

Civil Money Penalties for Violations of the Bank Secrecy Act (BSA)



UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:)
) Number 2021-01
The Kingdom Trust Company)
Murray, Kentucky)

CONSENT ORDER IMPOSING CIVIL MONEY PENALTY


The Financial Crimes Enforcement Network (FinCEN) has conducted a civil enforcement investigation and determined that grounds exist to impose a Civil Money Penalty against The Kingdom Trust Company (Kingdom Trust) for violations of the Bank Secrecy Act (BSA) and its implementing regulations.¹ Kingdom Trust admits to the Statement of Facts and Violations set forth below and consents to the issuance of this Consent Order.

I. JURISDICTION

Overall authority for enforcement and compliance with the BSA lies with the Director of FinCEN, and the Director may impose civil penalties for violations of the BSA and its implementing regulations.²

At all times relevant to this Consent Order, Kingdom Trust was a trust company organized under the laws of the state of South Dakota and therefore a "bank," as defined by the BSA and its

¹ The BSA is codified at 12 U.S.C. §§ 1826, 1951-1960; 31 U.S.C. §§ 5311, 5314, 5316-5330 and includes other authorities referenced herein. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.
² 31 U.S.C. § 5321(a); 31 C.F.R. §§ 1010.810(a), (d); Treasury Order 180 (July 1, 2014, reissued Jan. 14, 2020).



UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:)
) Number 2021-01
Capital One, National Association)
McLean, Virginia)

ASSESSMENT OF CIVIL MONEY PENALTY

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalty against Capital One, National Association (CONA or the Bank), pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to the BSA.


CONA has admitted to the facts set forth below and that its conduct violated the BSA. CONA has consented to the assessment of a civil money penalty and entered into a CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY (CONSENT) with FinCEN. The CONSENT is incorporated into this ASSESSMENT OF CIVIL MONEY PENALTY (ASSESSMENT) by reference.

JURISDICTION

At all times relevant to this ASSESSMENT, CONA was a "financial institution" and a "bank" within the meaning of the BSA and its implementing regulations.² FinCEN has the authority to impose civil money penalties on financial institutions, including banks, that violate the BSA.

¹ The BSA is codified at 12 U.S.C. §§ 1811-1814, 1816-1830 and 12 U.S.C. §§ 1826, 1951-1959. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.
² 31 U.S.C. § 5321(a); 31 C.F.R. §§ 1010.810(a), (d); 1010.1000(i).
³ 31 U.S.C. § 5321(a); 31 C.F.R. § 1010.810(c).

- 1 -



UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:)
) Number 2021-03
Community Bank of Texas, N.A.)

CONSENT ORDER IMPOSING CIVIL MONEY PENALTY

The Financial Crimes Enforcement Network (FinCEN) conducted a civil enforcement investigation and determined that grounds exist to impose a Civil Money Penalty against Community Bank of Texas, N.A. (CBOT or the Bank) for violations of the Bank Secrecy Act (BSA) and its implementing regulations. CBOT admits to the Statement of Facts and Violations set forth below and consents to the issuance of this Consent Order.

I. JURISDICTION

Overall authority for enforcement and compliance with the BSA lies with the Director of FinCEN, and the Director may impose civil penalties for violations of the BSA and its implementing regulations.

At all times relevant to this Consent Order, CBOT was a "bank" and a "domestic financial institution" as defined by the BSA and its implementing regulations.³ As such, CBOT was required to comply with applicable FinCEN regulations.

¹ The BSA is codified at 12 U.S.C. §§ 1811, 1814, 1816-1830 and 12 U.S.C. §§ 1826, 1951-1959. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.
² 31 U.S.C. § 5321(a); 31 C.F.R. §§ 1010.810(a), (d); Treasury Order 180(a) (July 1, 2014).
³ 31 U.S.C. § 5312(b)(1) (defining domestic financial institutions); 31 C.F.R. § 1010.1000(d) (defining bank).

Source: FinCen: https://www.fincen.gov/news-room/enforcement-actions?field_date_release_value=&field_date_release_value_1=&field_tags_financial_institution_target_id=660

Without over-simplifying the complexities of banks' middle and back-office functions, all of the above can be avoided with software which is already available. With any model, the risk of garbage in, garbage out remains but AI, technology and software can make this far easier to spot and prevent.

SAAS: SOFTWARE AS A SERVICE, SOFTWARE AS A SOLUTION

Some typical examples of BSA violations identified in correspondent banks are set out on the next page as a reminder of the current state of play. In the most extreme cases, the powers that the Secretary of the Treasury has under Section 311 of the USA PATRIOT ACT may be brought to bear are also detailed.

The reasons for the violations, their simplicity and the ease of fixes, all come down to automation. Software as a Service (SaaS) is a widely accepted, global acronym. In this case, whether cloud-based or not, software is also the solution.

COMMON BSA VIOLATIONS



- Failure to Develop and Implement an Effective AML Program
- Failure to File Suspicious Activity Reports

The Bank was notified that it was in violation of the BSA, including for failing to develop and implement an effective AML program that met the minimum requirements of the BSA or the FDIA and for failing to file SARs in accordance with BSA requirements.



- Failure to File Suspicious Activity Reports
- Failure to Document Decisions Not to File SARs
- Failure in Due Diligence of Correspondent Banks

The Bank failed to file Suspicious Activity Reports in 2017 and 2019; OCIF examined Bancrédito and cited it for additional BSA violations, including failures to file SARs, failures to document decisions not to file SARs, and failures related to due diligence on correspondent accounts for foreign financial institutions, among other AML program deficiencies.



- Over-use of 'Exemptions' to Lower Case Load and Alerts

The Bank's automated AML monitoring system generated a substantial number of case alerts on potentially suspicious activity. To reduce the number of case alerts AML staff had to review, the BSA Officer applied exemptions for customers whose activity was thought to be "well-known," including those individuals later arrested for or convicted of financial crimes, which resulted in lowering the case alerts generated for those customers.



- Underdeveloped Process for Identifying and Reporting
- Reliance on a Single Employee for Daily Manual Review
- Failure to Recruit Sufficient Experienced Compliance Personnel

Kingdom Trust's process for identifying and reporting potentially suspicious activity during the Relevant Time Period was severely underdeveloped and ad hoc, resulting in Kingdom Trust's willful failure to timely and accurately file SARs Kingdom Trust relied on a manual review of daily transactions by a single employee to identify potentially suspicious transactions. These deficiencies were exacerbated by Kingdom Trust's failure, during the Relevant Time Period, to recruit sufficient personnel with experience in AML compliance.



- Significantly Understaffed
- Over-Reliance on Third-Party Contractors
- Failure to Train, Recruited Underqualified Contractors

The Bank relied on third-party contractors to augment staffing levels. In 2018, the Bank conducted an assessment and determined that it needed 178 permanent, full-time positions to fully staff its compliance functions. As of early 2021, the Bank had 62 vacant positions, including the head of the Bank's Financial Intelligence Unit (FIU). Additionally, USAA FSB supplemented approximately 76% of its compliance staffing needs with third-party contractors. However, the Bank failed to properly train or otherwise ensure these contractors possessed satisfactory qualifications and expertise.

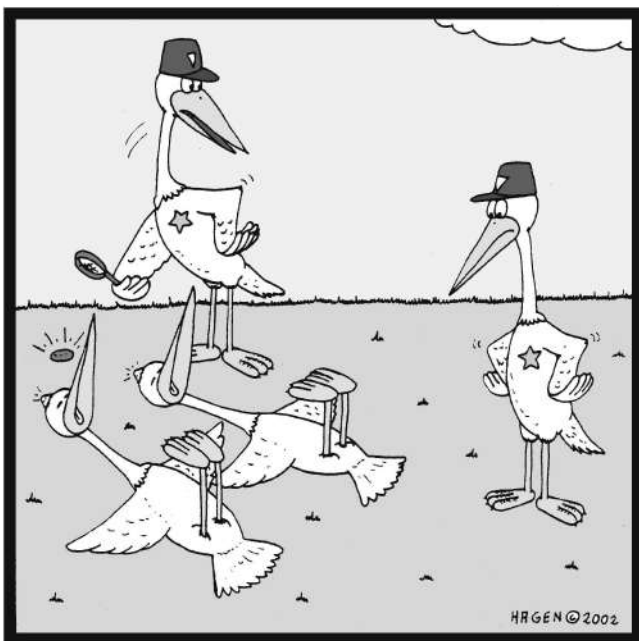
Trust Between Regulators & Banks Can Easily Be Improved

Establishing trust and verifying data is at the heart of cross-border payments, with authentication and confirmation techniques central to KYCC (knowing your customer's customer).

Until now, neither the technology nor the collaborative desire across stakeholders to enable a payments infrastructure across borders has been available. Diverse political interests and regulatory disharmony across accounting and regulatory regimes have previously rendered this ideal little more than a pipe dream. Building trust between regulatory authorities and correspondent banks is fundamental to the evolution of cross-border payments. This is often overlooked as an area to tackle, and understandably so, because it is not easy.

KILL TWO BIRDS WITH ONE STONE

The lack of comfort and belief that the banking industry has that it can correctly interpret and implement the required risk-based systems, across multiple jurisdictions, is primarily to blame. Infrastructure that could provide the building blocks of this has not, until now, been created because too many stakeholders want a say.



Unbelievable! It looks like they've both been killed by the same stone...

A successful cross-border payments system into the U.S. will require a dynamic, rules-based and artifact-rich (digital documentation, third-party authentication) process. In a best-case scenario, this will also provide “see-through” transparency of full disburser KYC details and all KYT documentation for the correspondent banks, the payment channels, the originators and the central banks.

“

“The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.”

BILL GATES

New technology, though not yet widely adopted, already makes it possible for a U.S. correspondent bank to either “accept and trust” the results and checks of an inbound transaction, or actually execute a re-run of all KYC, KYT and AML processes. In the first case, all foreign KYC, eIDV, AML, sanctions and other checks can be included in an authorization routine for 100% of all inbound transactions.

That is a new standard of transparency, but there's more. Technology now can enable the U.S. correspondent bank to run KYCC checks itself, instantaneously, with all the artifacts at hand. The bank can then apply its analytics to decision this transaction. It's difficult to imagine a regulator who wouldn't welcome this process.

Combining all of the above technology with improved communications (see 1 Suggestion) can, in one fell swoop, kill two birds with a single stone.

Did You Know?

Globally, only 54% of wholesale payments go from originating bank to end-customer's account within one hour.

2 PREDICTIONS

Software Solutions Will Cut Costs by 50%, Violations by 90%

One of the least well understood components of the de-risking challenge is how much the burden of increased compliance and checks actually costs. Lack of profitability is cited widely as a reason to step out of the game, but little data is readily available.

Per nostro account (see *Crossed Wires* section), a fair estimate is that the cost has risen from “who cares—it’s a cost base, loss-leader as part of our broader service” in 2000, just prior to 9/11, to about \$25,000 earlier this decade.

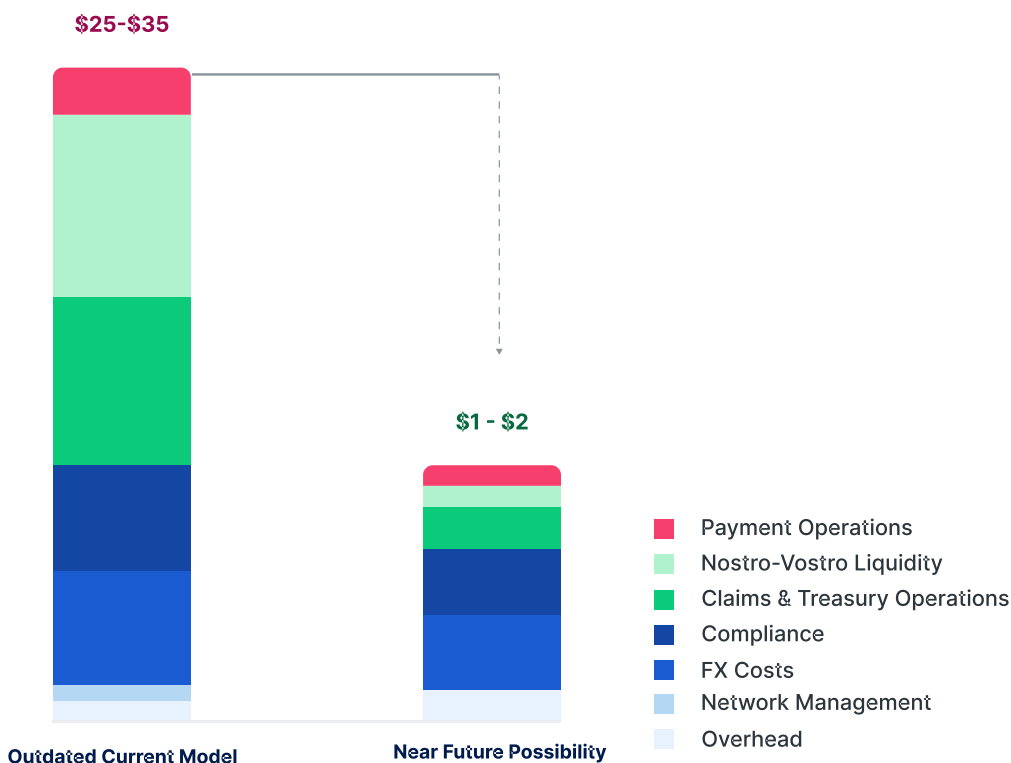
SOFTWARE MAGNIFIES THE BEAUTY OF OPERATING LEVERAGE

A fixed dollar-cost per account, where revenues from that nostro account will often fail to match the expense drag, is an unappealing loss-leader for service at best, and an open-ended liability at worst.

When considering how valuable a cross-border payments system that works would actually be for a correspondent bank, the economics are convoluted but highly compelling. The benefits of scale are quickly seen in a rising operating margin as volumes grow, and the risk-based capital drag falls away as AML and CFT risk is mitigated by software.

Throw in a dramatic fall in the personnel and man-hours required once end-to-end, see-through transparency and reporting are delivered, and a halving of these costs per relationship is only the beginning. Once the correspondent bank begins to grow this line of business again, secure in the knowledge that the risk is now being managed, the operating income grows far more quickly than expenses, and the margin expands.

Costs of Cross-Border Payments



Source: McKinsey, 2018: <https://www.mckinsey.com/-/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20vision%20for%20the%20future%20of%20cross%20border%20payments%20final/A-vision-for-the-future-of-cross-border-payments-web-final.ashx>

Rather than having to add additional compliance personnel steadily as the flow of business grows—effectively a steady fixed-cost highly unappealing to most banks—successful software and reporting automation becomes a source of operating leverage.

NO NEED FOR DEFENSIVE FILING = WIN-WIN

As to how a software solution can lower the number of violations, as well as the FinCEN and regulatory workload, the upside is abundantly clear. The removal of human error from each step of the onboarding and verification process, with checks and balances automated, coupled with the regulators' ability to interrogate transactions in real time and monitor and check artifacts, will all but eradicate the most egregious of human errors. We estimate that 90% of violations will be avoided, but the reality could be higher.

End-to-End Visibility Becomes Available to Regulators

Correspondent banks that choose to implement successful software and automation infrastructure to harness the power of digital capture, AI and all that software can now do, will use this new-found transparency and visibility to prove to regulators that they are doing everything possible to manage risk, rather than avoid it.

This renders KYT and KYC see-through very powerful. But KYCC—the ability to re-run checks using one's own tools and rules versus trusting the results of others; end-to-end tracking of real-time and historic payments across currencies all the way back to the ultimate beneficial owner—is the real game-changer. When combined with real-time analytics and decisioning on 100% of all transactions, it's very hard to envision a better way to protect cross-border payments. Somewhat intriguingly, this is actually possible through an architectural construct central banks already know well—a single-shared platform—but one that is adapted to carry more than just gross or net settlement details. This new platform, effectively a global shared platform, can carry KYC, KYT and much more data than previously believed.

AUTOMATION/DIGITIZATION WILL TICK MANY ENFORCEMENT BOXES

Once the Secretary of State determines that a foreign financial institution is of primary money laundering concern, the Secretary has the authority to require domestic financial institutions and financial agencies to take certain special measures against the entity of primary money laundering concern.

These special measures range from requiring additional due diligence and special attention concerning particular account transactions to prohibiting the opening or maintenance of any correspondent or payable-through accounts. A cursory glance at the roster of measures that can be enforced again confirms one truth—automating and digitizing data at the choke points of money flows would be a powerful addition to the regulatory arsenal.

- Record keeping and reporting certain transactions;
- Collection of information relating to beneficial ownership;
- Collection of information relating to certain payable-through accounts;

PLUG AND PLAY FOR ENFORCEMENT AND REGULATION

The simplicity of many of the errors made and the common themes—in most cases, lack of manpower and lack of experience—can all be alleviated by rules-based software. Start with the low-hanging fruit and plug into the software to enhance enforcement agencies' ability to screen, slice and dice and monitor payments flows into the U.S.



FINANCIAL CRIMES ENFORCEMENT NETWORK

FinCEN Finds Iraq-based Al-Huda Bank to be of Primary Money Laundering Concern and Proposes a Rule to Combat Terrorist Financing

Immediate Release: January 29, 2024

Source: FinCEN: <https://www.fincen.gov/news/news-releases/fincen-finds-iraq-based-al-huda-bank-be-primary-money-laundering-concern-and#:~:text=Home%20Finds%20Iraq%2Dbased%20Al%2DHuda%20Bank%20to%20be%20of%20Rule%20to%20Combat%20Terrorist%20Financing>

- Collection of information relating to certain correspondent accounts;
- Prohibition or conditions on the opening or maintaining of correspondent or payable-through accounts.

1 SUGGESTION

FinCEN Can Ease Tensions by Sharing More Information

Jeff Ross' insights into this issue were enormously helpful in shaping the law enforcement and regulatory perspective in this paper. His 30-plus years of public and private sector experience in AML compliance, began in the early 1990s in the U.S. Department of Justice's newly created Money Laundering Section, FBI's post-9/11 2001 Terrorist Financing Operations Section. His tenure concluded in 2008 with the U.S. Department of the Treasury's Office of Terrorist Financing and Financial Crimes. For the next 11 years, Ross served as the Senior Vice President for AML Compliance at Green Dot Corporation, a FinTech bank holding company, as well as at Green Dot Bank.

In Ross' opinion, FinCEN can be more transparent with those it regulates. "I do not think FinCEN has been as transparent, historically, as it should with its regulated entities ... Although FinCEN publishes information at the most basic level regarding, for example, investigations, indictments or convictions assisted by BSA filings, and chairs the Bank Secrecy Act Advisory Group, more needs to be done, as it was after the events of 9/11 to discuss and address larger issues, such as de-risking."



"FinCEN is in a unique position to issue more targeted and detailed FinCEN Advisories describing what law enforcement and FinCEN are seeing in a given area. For example, cross-border movements of funds with sufficient information to assist the banks and others affected to take counteractions ... To warn a bank or financial system, 'This is what we're seeing.' In other words, take the cards you're holding against your chest and actually let them out a little bit, maybe at least let them see the suit if not the number on the card."

JEFF ROSS, BSA/AML/OFAC/CTF
COMPLIANCE EXPERT

One Suggestion

De-Risking Cross-Border Payments:
Software vs. Sledgehammer
Jonathan Tyce interviewing Jeff Ross

00:00 43:05

JEFF ROSS
BSA/AML/OFAC/CTF Compliance Expert

A key aspect of addressing the de-risking challenge is to rebuild trust, and in some cases, relationships between the regulator and regulated. Again, Ross' suggestion for one way to kick-start that is simple. If law enforcement and FinCEN viewed part of their role as actually to help the banks identify issues and, periodically, stopped to thank the banks for all that they are filing, progress could be smoothed.

Did You Know?

Globally, 24% of retail services take more than one business day to make funds available to the receiver.

CROSSED WIRES: WHY DOES DE-RISKING HAPPEN?









“If you define the problem correctly, you almost have the solution.”

STEVE JOBS

The majority of the reasons that de-risking continues to occur are well documented. That said, limited headway has been made in recent years toward resolving these as the plethora of challenges—war, technology, digital currencies—shift and grow. The failure to identify, agree and work on common ground across the various stakeholders’ interests is also largely to blame.

COMMON REASONS TO AVOID RISK VS. MANAGE RISK

 Profitability Concerns	 Reputational Concerns	 Lower Risk Appetite
 Failure to Apply a Risk-Based Approach	 Fear of Supervisory Action	 Improper Implementation of Requirements

To avoid rehashing a well-rehearsed debate, this paper will adopt a somewhat typical focus to explore why de-risking happens. The lack of profitability in correspondent banking and the confusion and lack of clarity surrounding risk-based guidance are critical.

THE CHANGING ECONOMICS OF CORRESPONDENT BANKING

Profitability concerns that drive banks to opt out of the cross-border payments industry are widely cited, but finding numbers to quantify the reality is not easy. However, once a ballpark for the explosion in costs can be established, and the financial risk of getting it gravely wrong in a post 9/11 world is added in, things look very different.

A RISK WORTH TAKING?

Putting the issue of financial penalties to bed early, and even though instances of getting it this wrong are few and far between, the potential size of fines versus the potential revenue rewards will drive further de-risking. This will not change until human error and bad actor risk can be mitigated—ideally with technology.

01 BNP Paribas’ Money Laundering—\$8.973 B	09 Wells Fargo & Rampant Mismanagement—\$3.7 B
02 The AML Program That Wasn’t—\$1.256 B	10 Credit Suisse’s Toxic Asset Sell-Off—\$5.3 B
03 The MAN Group’s Poor Trading Oversight—\$1.312 B	11 Goldman Sachs & the Pilfered Malaysian Coffers—\$5.4 B
04 JPMorgan Chase & the Biggest Ponzi Scheme—\$1.7 B	12 Deutsche Bank & SMC—\$7.2 B
05 SAC Capital Advisors & Insider Trading—\$1.8 B	13 Binance Violates the Banking Secrecy Act—\$4.3 B
06 Credit Suisse & Tax Fraud—\$2.5 B	14 JPMorgan Chase & SMC—\$13 B
07 LIBOR Price-Fixing Scandal—\$2.5 B	15 Bank of America & SMC—\$30.6 B
08 Wells Fargo’s Phantom Accounts—\$3 B	

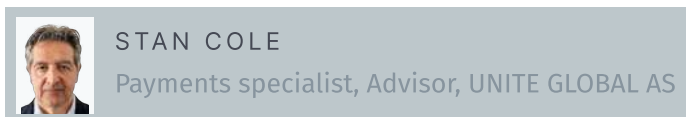
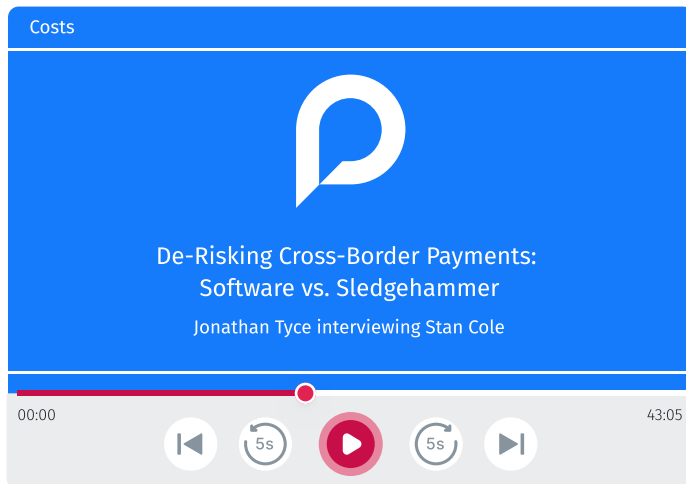
Source: Enzuzo, 2023; <https://www.enzuzo.com/blog/biggest-compliance-fines>

For most midsize U.S. correspondent banks, the list of fines levied would destroy a reputation and in many cases, imperil solvency. Not a primary driver of de-risking, granted, but it’s hanging over the business for smaller players.

COST PER NOSTRO ACCOUNT—FROM ‘WHO CARES’ TO \$25,000

Tracing the pace of de-risking—with 9/11 a key turning point and the 2008-09 GFC a powerful catalyst—the order of magnitude of the rise in costs and fall in profitability for correspondent banking becomes all too clear.

Back in 2000, the front-end client relationship-management role of correspondent banking was very unlikely even to have a compliance officer or function in the unit. Stan Cole, a payments expert with more than 20 years working directly in correspondent banking, describes the sea-change in the cost base and appeal of cross-border payments for a bank from before 9/11 to now.



“Back when I started in correspondent banking, in 2000, I remember that the thinking was ‘yes, there are costs but no one was even looking at that time. It was like you don’t look at that, you just need to have international cross-border payments, you have to have a network of correspondent partners, and this cost was effectively buried in the general ledger.’ There would be somebody sitting in a back office who you didn’t know about,” Cole explains.

“Suddenly [after 9/11] they were on the floor, literally in the next cubicle, somebody

who is only looking at that aspect. And then these people are on payroll, they become a cost center.”

By 2002-2003, the cost per nostro account would have been clearer to understand with the heightened scrutiny of the business and reckoned to be in the \$8,000 to \$10,000 range.

“As time progressed, leap forward to about 2020, the average cost for a nostro account for a bank in the U.S.—was somewhere in the neighbourhood of \$25,000.” This dramatic acceleration was fueled by a litany of global events—the Iraq War, the 7/11 attacks in London and other terrorist events, all of which Cole can directly map onto further cost pressures and scrutiny on the business.

RISK-BASED CONFUSION AND CROSSED WIRES

USA PATRIOT ACT



Why a bank would chose to avoid risk rather than manage it, and how regulators and enforcement agencies can help resolve this problem are key.

This decision—often based on a lack of trust and clarity about the risk-based approach parameters—effectively creates the same unintended consequences in the system as the risk of spiraling costs and fines do, but for very different reasons.

SUSPICIOUS AND UNUSUAL = TENSIONS

In the AML context, the tensions between the regulators and the regulated have existed for at least the 30-plus years of Ross’ considerable experience, and almost certainly longer. And they are inherent because the fundamental question has to be based upon what appears “suspicious” and “unusual.”

This Section allows for identifying customers using correspondent accounts, including obtaining information comparable to information obtained on domestic customers and prohibiting or imposing conditions on the opening or maintaining in the U.S. of correspondent or payable-through accounts for a foreign banking institution.

Source: FinCEN.gov: <https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act>

“I remember this from the 1990s—we’d be sitting in a BSA AG meeting and the banks would be there,” he recalls, “and they would say, ‘We want clarity. We want you to tell us what we shouldn’t take. Tell us the bad countries, tell us the bad actors, tell us this, tell us that.’”

And in response, Treasury and Justice would come back and say that they couldn’t do that, primarily because the bank was the one moving the funds, the bank was the one impacting the global financial system and the bank was the one making the decision as to whether to take on a correspondent relationship or not.



“9/11 changed a lot of that. After the shock of 9/11 the USG and its AML regulators became more prescriptive, particularly in a PATRIOT ACT Section 311 ‘Special Measures’ context at Treasury, where Treasury can and does actually tell the U.S. financial system, for example, ‘Cut off correspondent relationships with X, Y, Z.’”

JEFF ROSS, BSA/AML/OFAC/CTF
COMPLIANCE EXPERT

A 3-11, once considered something of a death sentence for a foreign bank or a foreign company’s intention to trade with the U.S., has lost some of its impact. Arguably, workarounds employed in recent years have rendered some of these sanctions less effective than they used to be. The over- or under-use of sanctions in this arena is not within the remit of this paper but clearly a relevant piece of the puzzle.

THE U.S. CHALLENGE

The realities of why de-risking actually takes place are, as detailed above, almost shockingly simple. Looked at from the perspective of U.S.-based correspondent banks supporting payments from overseas into the U.S., the

challenges and risks to cross-border payments are clear.



Research Note

International perspectives on de-risking

Perceived or assessed risk and adjusted risk appetite

Financial institutions often assume that customers of sectors or groups perceived as at high risk of money laundering or other financial crime present a higher individual risk.

Banks interviewed by the US Department of Treasury stated that they tend to avoid certain customers if they determine that a given jurisdiction or class of customer could expose them to heightened regulatory or law enforcement action absent of risk management.

Source: FCA Research Note, *International Perspectives on De-risking*, Sept. 2023

Many banks choose to simply avoid cross-border payment risks rather than endeavour to manage them. A cost-driven lack of profitability; a lack of clarity around implementation of risk-based approaches (as per the Bank Secrecy Act); and fear of fines and reputational damage are the most common causes.

From a regulatory perspective, reasons to “de-risk” a bank are more often than not down to a simple failure to implement and execute policies and procedures, either by the U.S. clearing institution or the foreign initiator of the payment. These are explored via real examples in the pages that follow. Best practices are already established but as yet unimplemented.

2 OVERLOOKED UNINTENDED CONSEQUENCES

Perhaps more importantly, de-risking a bank doesn’t—in the majority of cases—actually de-risk the U.S. payments system. Instead, AML/CFT risk is simply shifted to another channel, very possibly an unregulated one. Best practices can be established and implemented in 2024 and beyond in ways that were not possible even two or three years ago.

Further, regulatory de-risking of banks removes the pressure from those still in the business to invest and innovate, limiting the competitive pressure that usually drive efficiency and lower costs for customers.

AUTOMATING TRUST & THE BIRTH OF SEE-THROUGH



“Automation does not need to be our enemy. I think machines can make life easier for men, if men do not let the machines dominate them.”

JOHN F. KENNEDY

In an ideal world, the high-risk nature of cross-border payments can be mitigated with real-time data and documentation. Digitally stored artifacts that are verified by trusted third-party sources (think Thomson Reuters, Equifax) can further enhance this process and replace the need for trust with certainty.

Customer Due Diligence Made Safe

Single shared platforms are already widely used by central banks globally to share payment information between their banks. Thinking bigger, a global, single shared platform that stores and routes all KYC and AML data, providing visibility and rules-based, real-time decisioning for 100% of all transactions—importantly for all stakeholders—is the ideal.

Imagine a world with end-to-end visibility, where all necessary data is available at the click of a button, and this can be re-verified and re-run instantly. Carpenters have for centuries used the old maxim measure twice, cut once. The same thinking can now be applied to payments.

IN AN IDEAL WORLD

Software empowering local clearing institutions and correspondent banks to directly execute verification of the data collection and checks run by foreign disbursers is now available. Critical steps in the process including sanctions checks, electronic ID verification of foreign owners, company directors and their commercial activities can be effected and validated instantaneously.

Real-time source of funds checks, automated due diligence checks and dynamic KYCC can be performed before the transaction is actually processed. The ability to see-through to the disburser’s KYC checks, and digitally register that these steps have been taken, is what software can do to replace the need for trust with the visibility and answers that regulators and enforcement agencies demand.



Fast processing of sanctions checks



Real-time and automated source of funds and due diligence checks



Digitally register that all these steps have been taken.



Dynamic KYCC is performed before the transaction is actually processed.

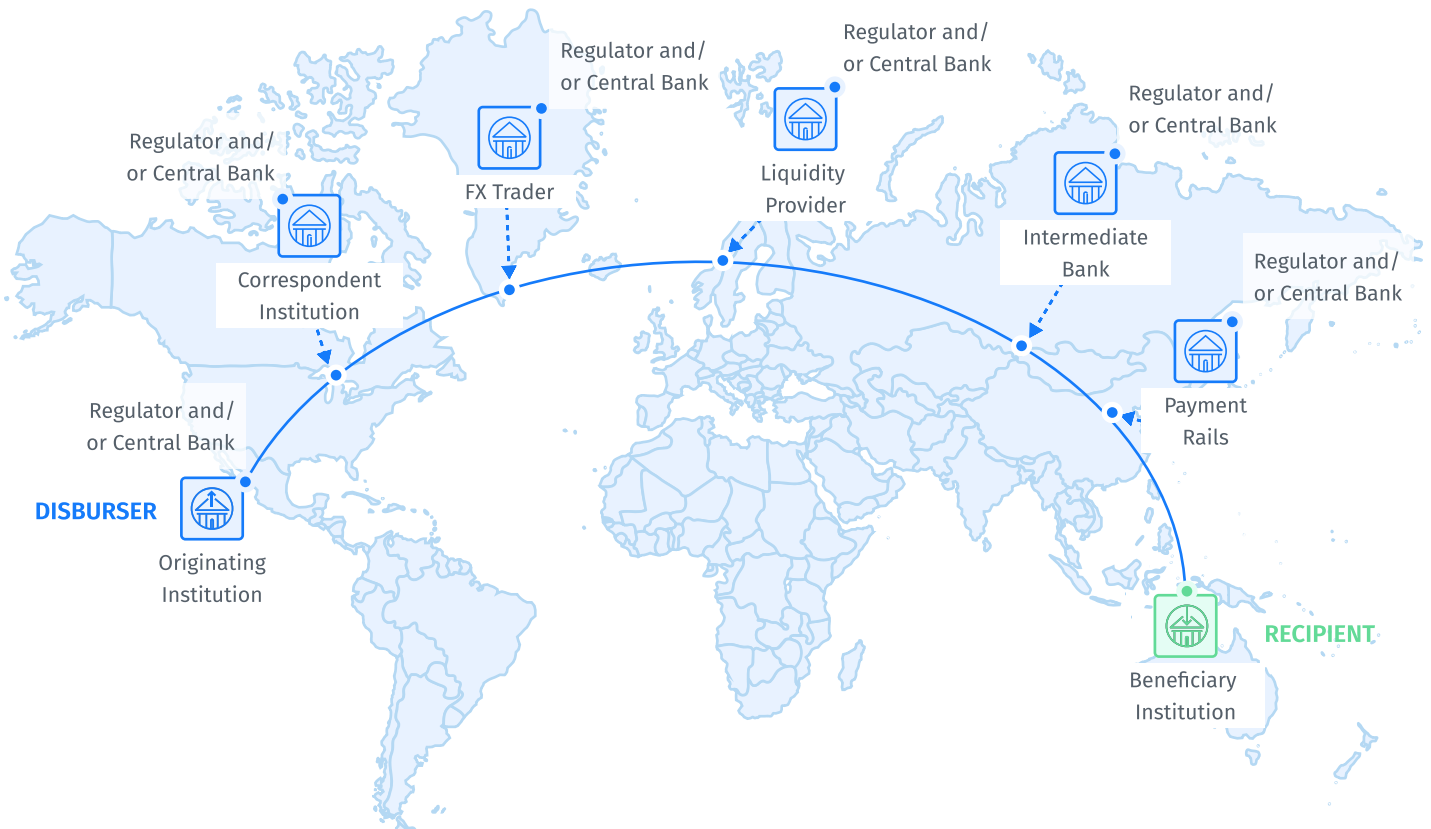


The ability to see-through to the disburser’s KYC checks



Electronic ID verification of foreign owners, company directors can be effected and validated instantly.

CONSIGN WILLFUL BLINDNESS TO HISTORY



SEE-THROUGH 'KNOW YOUR CUSTOMER'S CUSTOMER'



FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Action Task Force Identifies Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies

OFAC & FinCEN warnings are uniquely and specifically addressed

- ✓ Direct execution and decisioning of KYC, AML and sanctions check replace unverified "trust".
- ✓ Know Your Transaction **before** a payment is processed enables prevention.
- ✓ Complete "see-through" or Know Your Customer's Customer, with full KYC, AML and KYT document package

Willful blindness, itself an opaque concept that correspondent banks fear, will be banished to history with software and automated processes that confirm the three P's (policies, procedures and practices) are followed.

In civil enforcement of the Bank Secrecy Act under 31 U.S.C. § 5321 (a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the Bank Secrecy Act, or that the entity or individual otherwise acted with an improper motive or bad purpose. King Mail and A1 Duais admit to "willfulness" only as the term is used in civil enforcement of the Bank Secrecy Act under 31 U.S.C. § 5321 (a)(1).

Source: Fincen.gov, 2015: <https://www.fincen.gov/sites/default/files/shared/20150601Assessment.pdf>

SOFTWARE IS A NEUTRAL PLAYER



“No matter how good the system is, if it's not acted on, it's not worth anything.”

JEFF ROSS, BSA/AML/OFAC/CTF COMPLIANCE EXPERT

This paper has suggested that many of the unintended consequences of de-risking can be avoided altogether by accelerating the adoption of software and automation to eradicate the majority of reasons that banks are either de-risked or choose to avoid risk rather than attempt to manage it.

From enforcement agencies' desire to pinpoint terrorist threats and drug cartels' money laundering channels, to the Fed's need to oil the wheels of global trade and finance, the interests and goals of stakeholders' in the cross-border payments world are nuanced and not easily aligned.



“Best practice is already pretty well established but getting there is really hard.”

HENRY RICHOTTE, FINTECH INVESTOR, EX-DEUTSCHE BANK BOARD MEMBER, COO

This is one of the major reasons why limited progress has been made hitherto in the de-risking debate. Thanks to the advances in technology, and the advent of AI, it is now possible to use software as an interface between financial institutions, regulators and law enforcement. This will provide the longed for visibility and certainty that correspondent banks need to stay in the cross-border payments game. It will smooth the tensions between regulators and the regulated. And it will work because software is a neutral player.

JOIN THE FUTURE OF CROSS-BORDER PAYMENTS



At Payall, our vision is to enable financial institutions, payment channels and central banks to move money globally, safely and efficiently at the speed of data, so your customers can send money or make payments to anyone, anywhere—even if recipients are unbanked.

As part of that work, we are proud members of The Payments Association. Hear more from industry experts on the future of cross-border payments in The Payments Association's recent [whitepaper](#).

If you believe in a digital revolution for cross-border payments and want to join us at the forefront, let's talk.

Visit us at www.payall.com

or contact us at:

contact@payallps.com



ABOUT THE AUTHOR



JONATHAN TYCE | DIRECTOR, KENAZ LTD

Jonathan Tyce started working in Financial Services in 1995 and throughout his career has focused solely on the financials space.

From launching and running a pan-European financials hedge fund at JO Hambro Capital Management to 12 years helping build out Bloomberg Intelligence (based in UK and Hong Kong) and run the financials research, including Payments, his breadth of experience and industry contacts offer a unique mix. Having left the City in May 2023, he now works for himself, having founded Kenaz, a payments consultancy, and TriggerPoint Research, an Alpha Capture platform.

He graduated from St. Anne's College, Oxford University in 1995.

ABOUT THE INTERVIEWEES



STAN COLE | ADVISOR, UNITE GLOBAL AS

Stan Cole is a seasoned financial professional with 20+ years' experience working with financial institutions (FIs) in correspondent banking and fintech roles.

Stan's FI banking career with top five Canadian banks spanned portfolios of foreign FIs across multiple geographies in Europe, Middle East, and Africa (EMEA) and Asia Pacific (APAC) where he managed relationship and sales of payments clearing and trade financing to banks.

In 2017 Stan transitioned to the payments fintech industry, facilitating networking and opening partnerships with provider banks, and leading sales to FIs of alternative cross-border payment products.

Stan benefits from a broad cross-cultural competence through extensive international work and expat experience, including seven years in Singapore, two in Denmark, and two in Kazakhstan.



JEFF ROSS | BSA/AML/OFAC/CTF COMPLIANCE EXPERT

Battle-tested (33 years) and highly awarded, Jeff Ross is an expert in BSA/AML/OFAC/CTF matters.

Jeff was a senior advisor for over six years at the U.S. Department of the Treasury/Office of Terrorist Financing and Financial Crimes and Department of Treasury. There he advised and assisted Treasury Department policy-making officials on all law enforcement, regulatory and international matters relating to money laundering, terrorist financing, economic sanctions enforcement and other financial crimes.

Moreover, he provided policy guidance to the Office of Financial Assets Control (OFAC), Financial Crimes Enforcement Network (FinCEN), the Treasury Executive Office of Asset Forfeiture (TEOAF), and worked with the Internal Revenue Service concerning Bank Secrecy and Privacy Acts regulatory and enforcement functions.

He helped develop all Bank Secrecy and PATRIOT ACT regulatory requirements, including customer identification procedures, Suspicious Activities Report filings guidance, correspondent and shell bank requirements, foreign primary money laundering jurisdiction designations and implementation, and money service business-related regulations.

Payall Payment Systems, Inc.

Payall, the first-ever cross-border processor for banks, enables regulated financial institutions to move money safely at the speed of data.

Our mission is to make cross-border payments fast, compliant, and cost-effective with a suite of breakthrough automated compliance and risk management solutions that bring transparency to the historically opaque world of correspondent banking.

Cross-border payments enabled by our proprietary technology and processes run on a global single shared platform and use our novel "Know Your Customer's Customer" product. The platform includes core-like accounts for all users, with special-purpose payment processing representing "new rails" for near-instant and efficient global payments.

Moreover, cross-border payment recipients have unprecedented, valuable choices to access and manage their money, with payout options that appeal to financially savvy and unbanked individuals.

Contact us at:

www.payall.com

contact@payallps.com

