

WHITEPAPER

A beginner's guide to geopolitical risk, and how it's impacting fintech

March 2021

This Pareto Economics whitepaper is in partnership with



Contents

Executive Summary	3
About.....	5
From Bone to Bitcoin	6
Defining Geopolitics.....	6
Centres of Power (CoP)	7
The Great Convergence	8
The Fintech Landscape and Geopolitical Weak Spots	9
Geopolitics & Fintech: A closer Examination	11
Case Study: Fashion & Fintech.....	13
Sanctions Risk	14
Geopolitical Events and their Impact on Anti-Financial Crime Practice	15
Tax Evasion	15
Terrorist Financing.....	16
Money Laundering	17
Solutioning using Geopolitical Events	18
Practical Solutions using Geopolitical Analysis for Fintech De-Risking.....	19
Horizon Scanning	19
Reactive Analysis.....	20
Skillset and Strategic Approach.....	20
Risk Assessments	21
Case Study: Merchant Service Provider	22
Training	22
Outsourcing.....	23
Contact.....	24

Executive Summary

This White Paper is based on research and analysis undertaken by Pareto Economics and FINTRAIL.

Geopolitics is a phenomenon that is increasingly impacting the global fintech and financial services ecosystem. This is giving rise to a series of interconnected risks that are both new and difficult to mitigate, especially with the existing risk management frameworks.

The core conclusions from this whitepaper are threefold:

Firstly, fintech professionals especially in the risk management and business growth strategy space are lacking a robust and UpToDate understanding of geopolitics and globalised power and how they impact risk.

Secondly, those in leadership positions such as MLROs, CXO's, Management and Analysts need to have a more active and hands-on approach when assessing undiscovered and future risk to the business. A check box approach to risk management is not enough.

Thirdly, given the changing nature of world affairs, fintechs are experiencing a growing need to hire for geopolitical awareness and analysis skills and/or to seek outside assistance in order to properly hedge against an increasingly complex risk landscape. Most at risk departments include compliance, business strategy and operations.

The first section, ***"From Bone to Bitcoin"*** documents the evolution of fintech over its 20,000-year history from primitive forms of accounting to the digital assets of today,

giving much-needed context to the importance and development of financial technology.

Section two, ***"Defining Geopolitics"*** explains in a simple and useful way what geopolitical risk is and how it differs from political risk.

Section three, ***"Centres of Power (CoP)"*** introduces the reader to the concept of **globalised power** as well as the **developmental differential** and why the Centres of Power theory is a much better explainer of power structure and influence, using the US as an example of this theory in action.

Section four, ***"The Great Convergence"*** describes in a clear way how and why geopolitics becomes a dominant theme of change in today's world.

Section five, ***"The fintech Landscape and Geopolitical Weak Spots"*** distinguishes how geopolitical risk is not a one size fits all consideration. Its effect on fintech is dependent on the nature of the risk as well as the characteristics of the fintech itself.

Section six, ***"Geopolitics & fintech: A closer examination"*** dives in deeper into the relationship between geopolitics and fintech and with the help of two interesting case studies shows how geopolitics can impact the fintech market in very unexpected ways. Section seven, ***"Sanctions Risk"*** explores a more familiar compliance consideration, but

this time approaches it in a much more innovative and useful way.

Section eight, **“Geopolitical Events and their impact on Anti-Financial Crime Practice”** looks at three key geopolitical events involving tax evasion, terrorist financing, and money laundering that had a direct impact on anti-financial crime practice. Firstly, we'll review the circumstances and events around these three crime types that led to the realisation of new risks, and legislative changes to counter those risks.

Section nine, **“Solutioning Using Geopolitical Events”** addresses how fintech can inform and protect themselves from future risk by adopting integrated approaches between risk management and geopolitical analysis to help make the fintech ecosystem a hostile environment for those looking to exploit it.

About



The *Pareto Economics* helps clients understand and navigate complex and at times unprecedented risk brought about by the convergence of the Global 4 which includes: Globalisation, Geopolitics, Transformative Technology, and Societal Change. We do this through our leading research house and strategic consulting. We tailor each engagement with bespoke insights and actionable intelligence so that clients feel confident they are making the right investing, business and risk management decisions. (<https://pareto-economics.com/>)



FINTRAIL are a consultancy here to help you, your company, and your clients manage their exposure to the threat of financial crime and comply with any regulatory requirements. We're passionate about combating financial crime through the use of intelligent, commensurate, and inclusive programs working to disrupt criminal actors, whilst maintaining a best-in-class experience for your customers. We work with our clients to help them manage their risks through bespoke control frameworks, as well as providing subject matter expertise and training around financial crime laws and regulations and how to implement them in a way that works for you. (www.fintrail.co.uk)

From Bone to Bitcoin

From the first known human form of account keeping, the Ishango bone in 20,000 BCE, to representative money during the Mesopotamian era in 3000 BCE, to the use of standardised coinage in the form of small bronze knives and spades during the Zhou dynasty in China in 1000BCE to bills of exchange used by European traders in the Middle Ages to BankAmericard - the first payment card in 1958, digital money at the turn of the century and the advent of cryptocurrency in 2008; financial technology is a lot older than first thought.

The modern fintech stands on the shoulders of more than 20,000 years of innovation and development, and like fintechs of the past, they have got their fair share of risks to manage, mitigate and hedge.

Financial innovation has grown as a result of technological advancements, societal demand and the rise of global and more sophisticated trade. Naturally, as the world becomes more interdependent and interconnected so to do the risks, and in particular geopolitical risk.

For some fintech professionals, the main and perhaps only result of active geopolitical risk is the rising use of sanctions. Although sanctions implementations are an important result of geopolitics, they are not the only repercussion of rising geopolitical risk that fintechs need to be aware of. Other risks like money laundering, tax evasion and terrorist financing are also primary considerations.

The rest of this whitepaper will dive into what geopolitical risk is and why it seems to be so rampant in all parts of the world. We will then discover what risks fintechs face in this brave new world and how some have a reflexive relationship with geopolitics. Finally, we will discuss what fintech can do better when it comes to mitigating geopolitical risk.

Defining Geopolitics

The first place to start when understanding geopolitics is in the definition. Geopolitical risk is different to political risk, although a lot of the time many analysis and commentators mistakenly use both terms interchangeably. Political risk defines the risks and dynamics within the borders of a nation, whereas geopolitical risk describes the dynamics between nations. This distinction is evident in the insurance industry which specifically offers Political Risk Insurance (PRI) to companies operating in politically volatile regions. This kind of cover captures most, but not all, non-commercial risks which result from political events, including the direct and indirect actions of

POLITICAL RISK: The risks and dynamics which occur within the borders of a nation that can impact businesses.

GEOPOLITICAL RISK: The risks and dynamics that result between nations that can impact business.

host governments that negatively impact investments and are not properly compensated for, including: expropriation risk, currency inconvertibility, transfer restrictions as well as political violence like war, insurrection, rebellion, revolution, civil war, vandalism and sabotage¹.

Centres of Power (CoP)

To understand the rise of geopolitics one must first understand why and how globalised power is first created. Having a solid fundamental understanding of this will help the risk analyst develop a better understanding of the changing sands of world affairs, this will then allow them to make more confident, quicker and profitable investing and strategy decisions, as well as improve their ability to foresee and hedge risk.

A nations relevance and influence are predicated on developing, maintaining and leading in six primary interrelated and interconnected ways, what we call their "Centres of Power (CoP)". These include economic strength, active consumer market, production of systemically important resources, geostrategic positioning, technological leadership and military balance. Every nation, empire, kingdom and principality throughout history can be ranked against these six measures to determine their power and influence. Below are examples of how some countries rank in relation to these CoPs.



¹ MIGA WIPR REPORT, 2010. The Political Risk Insurance Industry. Chapter 3. [WIPR10ebookchap3.pdf](http://wipr10ebookchap3.pdf) (miga.org)

What is noteworthy to explore further is the United States visual. The characteristics of United States leadership which sees them take centre stage can be explained by their compounding development on all six CoP dimensions at a rapid rate which has solidified them as an unchallenged hegemon since the fall of the USSR in 1990.

Furthermore, as US power grew so did the dependency on the US by many companies and individuals. The US is also able to take advantage of this dependency by punishing rogue nations as well as financial and other business actors with sanctions as well as having the responsibility to enact strong and all-encompassing Anti-Money Laundering (AML) regulations with any individual or company who has a financial and/or business association with the US.

This example of extraterritoriality makes the US not only a geopolitically important nation but also by extension a global leader in the rules-based order. This title of the hegemon is being challenged as China develops its own CoPs to levels that also rival the United States.

The rise of globalised power in different parts of the world comes not from the US taking a “back seat” in world affairs, as some analysts have stated, but rather as the natural outcome in world affairs when nations begin to develop stronger CoPs to a point where they are able to have a bigger voice in regional/international affairs. The pie hasn't changed because the US is taking a smaller slice, it's changed because the pie has grown larger with more active players who have the financial capital to develop and pursue more ambitious regional and global agendas. The organic growth and reduction of nation's CoPs over time is what we have called the “developmental differential” and this more accurately describes the rise and fall of globalised power.

This is important for fintechs to know, especially when considering their risk controls and horizon scanning considerations for things like new market access strategies and how different jurisdictions are regulated, new money laundering corridors, changing sanctions landscape and what that means for business operations as well as your customer and customer's customer. Furthermore, changing consumer trends and innovating consumer products are also important condensations that emerge from properly understanding the rise of globalised power which taken together are essential for both business growth and sound regulatory protections.

The Great Convergence

As the developmental differential continues to compound with more nations now having diverse kinds of impact in their region and in the business ecosphere, four key themes have emerged over the years that have and will continue to impact and transform the fintech ecosystem. These “global four” themes include Globalisation, Geopolitics, Transformative Technology and Societal Change. It is the growing importance and interaction of the G4 with each other that has given rise to new fintech innovation, customer potential, financial crime risk and business growth opportunity.

As a standalone, these themes have always played an important role in the innovation of fintech. For example, the establishment of the first payment card was only possible because the technological innovation allowed it to exist, or the implementation of sanctions by the United States on hostile nations was a result of geopolitics.

What is unique about the time we live in now is that a convergence of the G4 is currently happening which is seeing complex relationships between the G4. This is giving rise to rapid and unpredictable change which is blindsiding regulators and fintechs, especially in relation to their compliance frameworks. What's more, due to these developments, fintechs now need to focus on upskilling as well as hiring for skills like triangulation analysis in order to meet these new challenges.

THE GREAT CONVERGENCE:

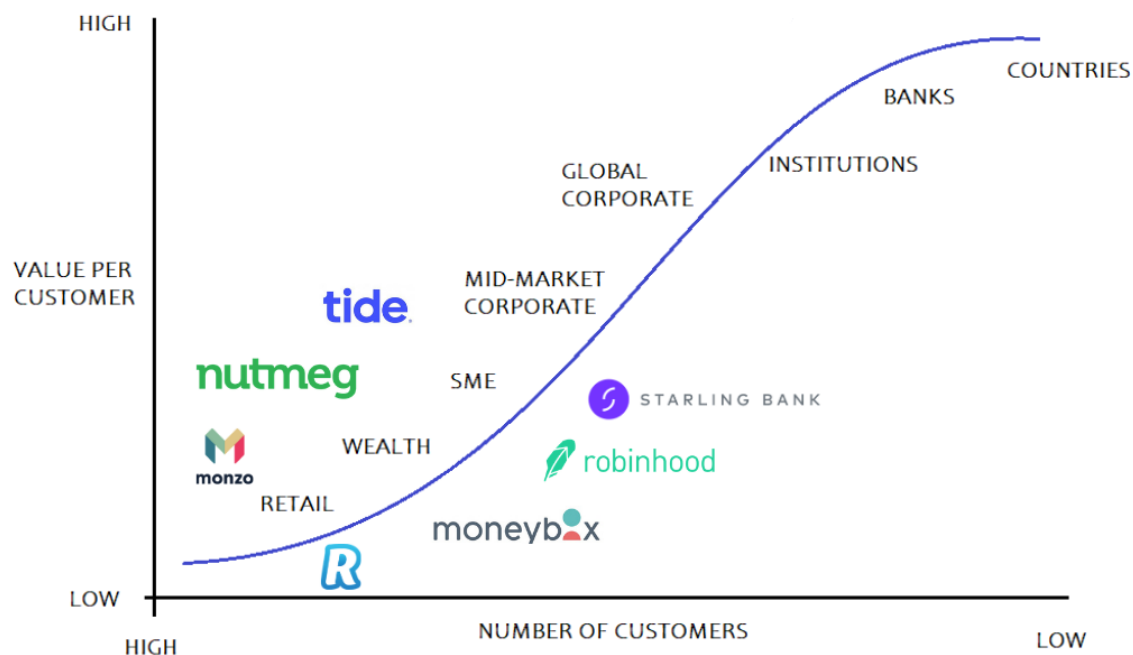
The change brought about by the interaction and interplay of the Global 4. (Globalisation, Geopolitics, Transformative Technology & Societal Change)

The Fintech Landscape and Geopolitical Weak Spots

Geopolitical risk is not a one size fits all consideration. Its impact on fintech is dependent on many factors that include; the characteristics of the fintech like its customer base (B2B/B2C), sector it serves and services it provides, size of its users, where it is based and the nations it operates in. As well as the service supply chain it is connected to, meaning a geopolitical risk can arise not only directly related to the fintech itself but also impact a fintech's customer and also its customer's customer. This non-linear thinking of geopolitical risk is what is needed in order for a fintech to see the full scope of risk and opportunity it faces on a daily basis.

The chart below describes the fintech landscape as it currently looks in the UK. Most of the activity and new business opportunities which have been established have tended to amass in the B2C space where the number of customers is high but where the value of each customer is low. Business growth for services like retail banking, wealth management, and the SME space has exploded over the years. Whereas growth in the B2B fintech market where the number of customers is low but the value per customer is high seems not to have sprouted much change and innovation.






The retail and wealth management space are interesting, especially as it relates to geopolitical risk. For example, the risks associated with prepaid cards like Revolut for illicit activity such as money laundering and terrorist financing is different to the risks associated with wealth apps like money box, nutmeg and plum which are also different to the risks associated with crypto assets. This is why horizon scanning coupled with product vulnerability testing is key to a more thorough and comprehensive risk-based approach to compliance and more holistic risk management.



Graph and concept courtesy of 11FS

The second dimension to geopolitical risk management pertains to the risks associated with the supplier landscape. That is to say, the fintechs that service other fintechs and financial institutions with underlying services like onboarding, KYC, sanctions screening, payments, banking as a service etc.

These software's, dashboards and tools can either be created in house or outsourced to vendors. Generally speaking, in regards to direct impact from geopolitics these suppliers have relatively little exposure, this is because they provide the "plumbing" for the ecosystem and are not on the frontlines, however, there are cases as we will explore later where these firms can be in the direct crosshairs of geopolitics. Where some fall short however is the risks they don't/can't target.

Supplier Landscape				
Onboarding	KYC	Sanctions Screening	Payments	Banking as a Service
	 BUREAU VAN DIJK A Moody's Analytics Company			

For example, a sanctions screening tool whether in-built or outsourced can do an excellent job detecting sanctioned entities and individuals, but it can't inform you of the changing geopolitical landscape that would prompt future potential primary or secondary sanctions to be implemented on a nation, entity or individual. This is especially important if a fintech/ financial institution was planning on expanding its reach into a seemingly "safe market".

Tools and metrics however are being developed by the Pareto Economics such as our Global Power Index which can be utilised by the compliance function, management, policy teams etc in fintech and financial services firms when assessing specific jurisdictions for a number of reasons including business growth, partnership risk and opportunities, 360-degree horizon scanning etc.

Geopolitics & Fintech: A closer Examination

As the phenomenon of globalised power continues to grow, two trends begin to emerge which have a distinct impact on geopolitics and also how geopolitics can impact fintech.

Firstly, population movements and migration patterns compound and become more unpredictable. This is due to a growing variety of factors including climate change, work opportunities, cheaper travel, forced migration due to war, poverty and civil unrest etc. This causes the social fabric of cities and countries to change in a variety of ways, which as a second-order effect means nations are tied closely to each other due to population dependencies.

Many examples exist of this including the migrant movements from North Africa and the Middle East to Europe, and movements of South Americans to the United States over the past few years, to Covid-19 allowing for remote working and mass repatriation of workers due to health and safety concerns. This also means fintechs need to be aware of these geopolitical changes especially because changing demographics impact compliance, operations as well as product-market fit.

The following case study highlights the secondary impacts that fintechs face in light of changing migration patterns.

Case Study: Indian IT professionals Post Brexit

Following BREXIT, the free movement of people from EU nations ended. This meant a more equal playing field was established for non-EU skilled workers from other parts of the world to compete for positions in the UK as the preferred treatment for EU workers was abolished. The Indian IT sector is poised to take advantage of this change due to BREXIT. With India's reputation as a technology hub and the fact that English is a primary working language for many, an influx of IT professionals may occur especially in the fintech space. This may then see a substantial increase of remittances take place which is set to benefit fintechs who focus or have exposure to Indian remittances like Western Union, Ria, Transfast and Xoom.

This also allows other challengers to vie for the same market especially if they have or can form partnerships with the companies who are attracting this new wave of workers.

Whereas most fintechs in the UK as it pertains to BREXIT may be thinking of issues in relation to FCA led changes including passporting restrictions, licencing and others. It is the ability to horizon scan in non-linear ways like this that will allow a fintech to truly be ahead of the curve.

Secondly, as this great convergence continues to evolve and impact more and more of society, what we will see arising is more industries that previously have never had to think of geopolitical risk now having it front and centre in their list of risk factors. This is because the world is becoming more globalised, which is allowing companies to expand into brand new markets in different parts of the world, as well as exploring new manufacturing bases which changes supply chains as well as other important factors in relation to compliance and operations. Some industries like oil and mining, however, have a much better grasp and appreciation of geopolitical and political risk as they have a history of operating in politically volatile emerging and frontier markets where they face issues in relation to sanctions, civil war, rebellion, strikes, riots, terrorism etc. Other industries however are less experienced, this has seen them in the crosshairs of geopolitical risk.

The following case study highlights how geopolitical risk has a business coupling effect between different industries, and again is another great example of non-obvious risk.

Case Study: Fashion & Fintech

The rise of China's active consumer market has seen an increase in salaries and living standards which has fuelled demand for mass-market goods and services. One of the biggest winners of this expansion has been western fashion brands like Burberry, Ted Baker, Zara, Diesel, H&M, and Chanel.

Reputation and brand management is a key variable for success in the fashion retail world. This is especially important when selling into foreign markets. The American fashion brand GAP was caught blind sighted by unexpected geopolitical risk in 2018 which is worth understanding.

GAP was forced to apologise when Chinese consumers responded with uproar to a t-shirt for sale which only displayed the map of mainland China and failed to include other territories like Taiwan, the South China Sea and South Tibet. This lack of geopolitical awareness led to a boycott of the brand by Chinese consumers and reputational damage to the brand and a drop in its stock price. In a statement GAP said it "sincerely apologised for this unintentional error". Furthermore, the company said it respects China's "sovereignty".

This should serve as a lesson to fintech for two main reasons as it pertains to business coupling.

Firstly, the business coupling effect takes action where the rise of one industry is also pegged to the rise of another. In the case of China, the growth of its active consumer market saw a rise in demand for western fashion due to rising wages, this growth was also pegged to a rise in wealth tech and financial retail services which served to manage and grow wealth for Chinese consumers who were buying these clothes. Naturally, if a foreign fintech were to compete with the Chinese market, this business coupling strategy should be implemented and triangulated along with geopolitical risk and a fintech's own strategy and ambitions in order to gain a much better understanding of the risks and opportunities.

Secondly, the business coupling effect also impacts fintech in a different way. Namely by association. Meaning the success of a fintech in a foreign or indigenous market can be pegged to the reputation of a partnering firm in the same or different industry. If a western fintech were to have a partnership of some sort with another western or non-western fashion brand that operates in China, negative press from the "offending partner" can potentially impact the fintech by association, causing its customer base to migrate to other platforms, or cause the authorities to intervene making business operations very difficult. This is why fintechs need to develop much better mechanisms in order to assess business risk and opportunity, especially as it pertains to business coupling in the face of geopolitical risk.

Sanctions Risk

In this section we will cover a more traditional compliance risk, that being sanctions. The following case study highlights the reflexive relationship between geopolitics and fintech.

Case Study: SWIFT's catch 22

When President Trump announced his maximum pressure campaign on Iran in 2016, this put many western financial services firms like SWIFT in a very difficult place. In the case of Iran, both the EU and the US disagreed on fundamental aspects of Iran's compliance to the JCPOA.

President Trump announced that any organisation doing business with Iran whether American or not would face the imposition of sanctions themselves if they continued to do business with Iran. Belgium-based SWIFT was caught in the crossfire as not only did they provide the fundamental infrastructure needed for banks to communicate payment orders with each other, the EU also introduced blocking regulations which essentially made compliance with American secondary sanctions illegal.

SWIFT's board of directors also faced the threat of asset freezes and travel restrictions if they didn't comply. Despite the impact on business and with no shot of an exemption, SWIFT reluctantly complied with the American request and cut all ties with Iranian financial institutions and companies.

The geopolitical risks in this example are threefold.

Firstly, historic international alliances are now fracturing due to the developmental differential and a changing power landscape. This is causing a less homogenous international sanctions regime to emerge because western allies, like the EU, US and now the UK due to BREXIT all have differing sanctions protocols, which is making compliance more complex and costly.

Secondly, it demonstrates the significance of fintechs like SWIFT who play such a crucial role in international banking. Their ability to connect and disconnect a whole country from the international financial community is a powerful thing. Typically, many organisations have a reactive approach to geopolitical risk, this is due to the fact that they don't spend time understanding wider risk management and as a result often make decisions based on pressure, and short-term thinking when faced with a politically sensitive incident.

Thirdly, geopolitical risk can also provide a big opportunity for challenger banks and suppliers who are increasingly able to point to the vulnerability of the international payments landscape brought on by globalised power, as they are dominated by legacy organisations who may present a "too big to fail" position in the eyes of governments and regulators. Being able to provide smaller, more nimble solution can be a big pull for customers who are frustrated with the inefficiencies and slowing innovation of the incumbents. Coupled with regulations like PSD and PSD 2 which allow for market entry of these challenger banks, the ability for smaller players to show they understand the changing nature of world affairs and can provide solutions in response can be a winning combination.

Geopolitical Events and their Impact on Anti-Financial Crime Practice

Geopolitics has a direct influence and impact on global financial crime, by shaping the threat landscape. Financial services are targeted every day by organised crime, political corruption, and terrorist actors across the globe with the goal of moving and hiding money gained through illegal activities.

As a result of geopolitical events and changing threats, we have seen a number of reactive changes in law and regulation, requiring financial institutions to verify the identity and understand the risks of the customers they do business with. However, there is also a resulting change in internal compliance teams and global anti-financial crime standards to push for a more proactive approach. Using geopolitical event-driven analysis is, therefore, crucial in the effective fight against financial crime. Fintechs must make sure anti-financial crime tools and controls are fit for modern-day threats.

In the first part of this section, we look at three financial crime types and examples of geopolitical events that have driven change in legislation or created the impetus for financial institutions to review their financial crime controls, frameworks, and services.

Though money laundering is the predicate offence in almost all financial crime, we look specifically at the use of Russian laundromats to enable laundering activities; as well as two lesser discussed crime types: tax evasion and terrorist financing, which are notoriously difficult to identify based on financial analysis alone.

In the second part of this section, we discuss practical solutions. We look at how to use geopolitical events and analysis to inform risk and control frameworks, ensuring risk mitigation strategies remain up to date and in-step with modern financial crime threats.

Tax Evasion

In April 2016 the Independent Consortium of Investigative Journalists (ICIJ) released approximately 11.5 million files from Panamanian law firm Mossack Fonseca detailing financial and legal information on their clients. These became known as the Panama Papers².

Interrogation of the Panama Papers by journalists and investigators alike revealed multiple incidents of Mossack Fonseca shell companies being used by wealthy individuals to sequester their fortunes and, in some cases, use those shell companies to engage in tax evasion, fraud, and evasion of international sanction and embargo programmes.

² <https://www.icij.org/investigations/panama-papers/>

In response, the UK Government passed a new law known as the Criminal Finances Act 2017 (henceforth, the CFA). The CFA worked to enhance existing AML laws within the UK by introducing new investigatory powers for law enforcement and creating the Corporate Criminal Offence, which placed liability on firms (including fintech) to have mechanisms in place to prevent the facilitation of tax evasion.

From the leak, it's obvious that tax avoidance and, in some cases, evasion was rife. It's unlikely that banks who had customers named in this leak were fully aware of their involvement in potential criminal activities due to the nature of secrecy surrounding tax havens like Panama and the Mossack Fonseca firm. In the wake of the event, it is likely that banks will have used this now public information to re-risk their customers as part of their customer risk assessment.

The information from the Panama Papers leak would have been used reactively during that re-risking exercise, however, it can also be used proactively to inform future risk assessments. For instance, using the leaked data as an adverse media data point or proactive search criteria during enhanced due diligence.

This is a perfect example of financial institutions using geopolitical event-driven data to inform their financial crime risk and threat assessments. Using the information will have given firms a different view of their risk, in particular the risk of tax evasion, and created an impetus to put controls in place to counter that risk.

Had it not been for this geopolitical event, criminal tax evaders would have been afforded a longer period of latitude to fly under the radar of the firms that they banked with.

Terrorist Financing

In November 2015, Islamic State terrorists carried out a coordinated attack at the Stade de France and Bataclan Theatre in the suburb of St-Denis, Paris, killing 130 innocent civilians just 10 months after the lethal Charlie Hebdo attacks in January 2014.

Investigations following the fatal attack identified that the terrorists used a series of anonymous prepaid cards³ to fund their hotels and other expenses in Paris in the 48 hours leading up to the November 13th attack.

The anonymity offered by certain prepaid card products is an extremely attractive quality for hostile actors looking to transport and spend money. They're easy to access and can be purchased almost anywhere in the world – the investigation following the Paris attack identified

³ https://ec.europa.eu/newsroom/fisma/item-detail.cfm?item_id=29693&newsletter_id=166&utm_source=fisma_newsletter&utm_medium=email&utm_campaign=Finance%20&utm_content=In%20the%20spotlight%20How%20the%20EU%20is%20combating%20terrorist%20financing&lang=en

that some of the prepaid cards used were purchased in neighbouring Belgium and brought to Paris.

Investigators identified similar terrorist strategies using anonymous prepaid cards in the preparation of the 2016 suicide bombings in the Belgian capital, Brussels. Terrorist actors cycled funds between prepaid cards in order to avoid detection from banks and law enforcement enabling them to use the funds to rent accommodation and even purchase material used to create the bombs used in the attack.

As a response, in 2017 the European Union introduced within their fourth iteration of a legislative instrument known as the Anti-Money Laundering Directive (AMLD) a legal requirement that any anonymous prepaid card issued by an EU member state cannot transact more than the value of €250 within a one-month period. Then, in 2018, the European Union went one step further and reduced that monthly transaction limit to €150 to continue to counter the growing threats posed by extremist actors.

The introduction of these limits by the consecutive AMLDs illustrate direct change as a result of a catastrophic geopolitical event and then iterative change to ensure regulatory provision remains commensurate with the evolving threats posed by terrorist actors as prepaid cards began to be identified as being more and more popular with hostile and terrorist actors.

That said, firms do not need to wait until a new control or restriction is made a legal requirement. Geopolitical events such as terrorist attacks can be used to inform risk assessments and control frameworks based on information released to the public during the course of investigations post-event. Given that we know terrorism relies on financing, following any attack banks should look at any information in the public domain on how the attack was facilitated (e.g. the use of prepaid cards) and whether their current control frameworks and risk assessments would enable similar activity. If the answer is yes, then the controls should be remediated to mitigate the opportunity for the product to be exploited by hostile or terrorist actors.

Money Laundering

One of the most talked about and recent geopolitical events involving large-scale money laundering is the Troika Laundromat⁴.

The Troika Laundromat is the name given to a network of 70 offshore shell companies that were used to move approximately £3.5 billion (\$4.6bn) from Russia to the West. These companies were operated by employees of the former Russian investment bank, Troika Dialog, which was bought by the now heavily sanctioned Russian investment bank, Sberbank CIB, in 2012.

⁴ <https://www.occrp.org/en/troikalaundromat/>

The shell companies involved were owned by a network of “nominees”, or rather, persons standing in for the ultimate owners of the accounts, creating a vast network of anonymity with multiple ties to transnational organised crime groups. The companies laundered money between companies in the network, and also between multiple bank accounts associated with single companies within that network commingling illicit funds with legitimate ones to make detection near impossible. It was estimated that funds cycled around the laundromat several times before eventually being exited into the global financial system as seemingly legitimate funds.

An investigation into the Troika Laundromat by the Organised Crime and Corruption Reporting Project (OCCR) and other media outlets revealed the dirty Russian money to be flowing all over the world, with links to major banks like Deutsche and Danske Bank, and to high-ranking officials and politicians across the globe.

After the details of the laundromat hit the media, financial institutions began scrambling their compliance teams to assess whether they had unknowingly enabled the laundering of funds through the Troika Laundromat. As banks involved began to be named, media and regulatory pressure began to mount against financial institution's shortcomings with regard to anti-money laundering (AML) controls.

As banks combed their client books looking for any links to the Troika Laundromat, the European Union introduced the 4th Money Laundering Directive which set out to start tightening AML controls across the EU with a specific focus on member states identifying and registering ultimate beneficial owners of privately held companies and directly calling out shell companies as an attractive vehicle to launder funds that banks should start considering in their due diligence processes.

The Troika Laundromat is just one of many similar schemes used by bad actors to launder criminal proceeds across the globe and is often used to illustrate the contemporary threat that money laundering poses across the globe.

As a result of this geopolitical event, banks were forced to take a hard look at their clients, and their associated control frameworks to remediate any gaps or links to the Russian money-laundering scheme.

Solutioning using Geopolitical Events

As outlined, the current geopolitics landscape is complicated and difficult to navigate. Fintechs across the spectrum (from start-ups to large challenger banks) tackle these challenges in different ways – and with varying degrees of quality and effectiveness.

For smaller start-ups, upcoming geopolitical challenges are often the last thing on their mind. The core issue for these firms is regulatory compliance to acquire necessary licenses or banking partnerships, as well as refining their product and scaling. In these cases, proactively monitoring the geopolitical landscape likely does not take place.

Whilst more established fintechs may have more capacity to tackle geopolitical challenges, their focus often remains regulatory compliance. Large fintechs will have a Compliance, Investigations and/or Financial Crime function, tasked with keeping up to date with regulatory changes and ensuring compliance with necessary requirements. This approach is targeted at tracking specific regulatory changes that have a direct impact on the business and will often not cover the geopolitical shifts sitting behind the regulatory change. The result is an approach that is more reactive than proactive and often lacking in useful geopolitical context for upcoming regulatory changes, or emerging financial crime threats.

In FINTRAIL's experience, the quality of these types of solutions also varies widely from fintech to fintech. Some firms may deploy a technology solution to scan for regulatory changes - with some success at spotting updates. Others may rely on an individual in the Compliance team to check for regulatory updates manually, on an ad hoc basis. Finally, some fintechs may not have a plan in place at all and rely on banking partners or third-parties as informants of regulatory changes.

Ultimately there is no one-size-fits-all approach and no 'right answer'. However, some approaches are more effective than others and there are some practical ways that fintechs can mitigate geopolitical risk.

Practical Solutions using Geopolitical Analysis for Fintech De-Risking

To build a strong and effective approach to geopolitical risk management, fintechs should first view solutions holistically. There is no single 'quick fix' or technology solution that can facilitate geopolitical and regulatory risk mitigation. Practical and effective solutions require a combination of technology solutions; analytical skillsets and strategic approaches within the Compliance, Investigations and/or Financial Crime Teams; dynamic risk assessment frameworks; and – where necessary – outsourcing any required expertise on specific events.

Horizon Scanning

To get a sense of the geopolitical risk landscape, fintechs should proactively scan for upcoming events that may impact their business. "Horizon scanning" is a well-known concept and is most often used when scanning for upcoming regulatory changes. Indeed, fintechs (and all financial institutions) are required to comply with changing regulation and, therefore, need to spot any upcoming changes.

However, our experience at FINTRAIL has shown that not many fintechs are able to 'scan' effectively and if they do, the scope focuses specifically on minimum regulatory changes and not necessarily the geopolitical context. Whilst this may help to facilitate regulatory compliance in the short term, it does not enable proactive geopolitical risk management in the longer term. To manage upcoming geopolitical changes, scanning should pick up on the wider contexts instead of simply the regulatory output.

In practical terms, 'scanning' can be conducted in many ways, fintechs should consider their options, depending on the business size, associated product risks, jurisdictional footprint and the business risk appetite. These factors should be used to determine the type of scanning that is

required and any particular focus areas. Scanning could then be conducted using a third-party tool, with specific search parameters being used to focus on areas of concern or particular relevance. Firms could also set up a number of specific Google alert search terms or conduct internal research exercises on a recurring basis, perhaps in advance of core governance forums.

At a very basic level, however, firms should not overlook the importance of encouraging general geopolitical reading and awareness within the Compliance, Financial Crime or Investigations Teams. This is a cost and time effective solution – and can play a crucial role in spotting upcoming geopolitical events when aligned with a 'speak up' culture. Whilst not a fool proof solution on its own, general discussion on geopolitical events will certainly help.

Reactive Analysis

Whilst looking ahead is important for upcoming changes, fintechs should also not underestimate the value of reactive analysis following geopolitical events. Data leaks, terrorist attacks and other adverse geopolitical events should be used as a litmus test against current risk and control frameworks.

Investigations, once declassified, are often published in the press – for example, the use of prepaid cards in the Brussels and Paris attacks – which should be used to assess whether the techniques used by hostile actors would have been identified by the current risk assessment and associated control frameworks.

In an even more practical sense, when details of adverse geopolitical events hit the press (such as the names of terrorist attackers etc), it would be prudent for FinTech Investigation and Compliance Teams to screen customer books for those named persons or associates in order to (1) ensure that they are not exposed to the risk that customer presents, and (2) be able to report crucial intelligence to law enforcement investigating those adverse events.

Similar to creating a horizon scanning mechanism, a mechanism should be created to quickly react to those adverse geopolitical events. FINTRAIL have seen this done through on-call rotas within Compliance and Investigatory Teams, as well as making designated persons available to be contacted by national law enforcement agencies if and when these adverse events happen.

Skillset and Strategic Approach

Going beyond general awareness, individuals sitting within the Compliance, Financial Crime and Investigations Teams should also have strong analytical skills. The role of the Compliance function is no longer to simply 'tick boxes', but to operate more as a risk advisory function. To fulfil this role, Compliance Analysts must be able to examine problems and assess the upcoming risks, as well as develop effective control solutions. In the geopolitical sphere, these teams should be aware of upcoming changes, have the ability to research and assess the impact of these changes, and present compliant solutions to the business.

Compliance, Financial Crime and Investigations Teams should also deploy a strategic approach to geopolitical risk analysis. The team must be able to step back from a geopolitical event or

trend and view it through the lens of their specific business and products. The geopolitical landscape is full of events and changes, many of which will not be relevant or have any impact on the business. Taking a strategic approach will ensure time is spent on mitigating risks that will materially impact the business.

Risk Assessments

Building on this strategic approach, the business should also view geopolitical incidents as dynamic risks that inform overall risk assessments. Geopolitical events, identified as part of horizon scanning efforts, should not be assessed in isolation, but examined in line with the business context and fed back into the business-wide risk assessment. It is crucial that risk assessments be viewed as a live document – not simply an annual compliance task – that are updated as and when geopolitical events alter or reframe particular risk scenarios. These changes should then stimulate discussion and analysis as to whether existing controls are still effective or new controls are needed to mitigate the risk.

Case Study: Merchant Service Provider

FINTRAIL recently worked with a Merchant Services provider (Company X) to build out their financial crime risk assessment. In this case, Company X offered merchant services to UK-based companies. Company X considered the risk from geopolitical events to be low – almost non-existent.

Whilst we agreed that the risk was low, geopolitical awareness was still critical when examining certain risk scenarios. For example, although Company X operated out of the UK and applied geolocation controls on merchants to prevent them from operating outside of the UK, there was still a risk that beneficial owners of merchants could be based outside of the UK – potentially in sanctioned countries. To effectively mitigate this risk, a control was built to screen beneficial owners through a third-party provider. From a geopolitical risk perspective, Company X then had to consider the changing UK sanctions framework as a result of Brexit and verify whether controls would still be compliant following the UK's exit from the European Union.

Company X also faced risks from merchants being coerced by organised crime groups to process payments and launder illicit funds on their behalf. Whilst instances were low at the time, the risk may increase with a shift in geopolitical trends forcing criminals to seek out new ways to make and launder money. New fintechs with immature control frameworks can also be an easy target for criminals. In this case, Company X had to implement effective transaction monitoring rulesets to spot unusual or suspicious transactions and effectively mitigate the risk of processing illicit funds. By maintaining an awareness of the geopolitical landscape and its impact on organised crime (particularly in the UK), Company X will also be able to dynamically update the risk scenarios and proactively adjust transaction monitoring thresholds if particular threats appear to rise.

Training

Including geopolitical risk as an element of anti-financial crime and compliance training is critical to developing a team that is equipped to proactively identify emerging risks, and also able to apply context to financial crime investigations.

It is likely that some element of geopolitical training exists already within FinTech training programmes within elements such as country risk or the ideology behind terrorist fundraising. However, it is worth capitalising on the importance of using geopolitical context in a dedicated training session that is up to date with recent geopolitical events that have impacted financial crime. This session should include the regulations that speak specifically to the intersections of geopolitical risk and financial crime, such as high-risk country monitoring or the importance of limits in high-risk products like anonymous prepaid cards.

Outsourcing

Finally, fintechs may also consider outsourcing deep-dive research into specific geopolitical events. Where there may not be in-house expertise, time or tools, outsourcing can be a fast and effective way to assess a particular geopolitical change. Before requesting this outsource work, however, fintechs should make sure the third-party has a full understanding of the specific product and business model – the research must be as targeted and as useful as possible.

Contact



Klisman Murati

Director, Pareto Economics

klisman.m@pareto-economics.com



Jessica Cath

Senior Consultant, FINTRAIL

jessica.cath@fintrail.co.uk



Mikey Morton

Consultant, FINTRAIL

michael.morton@fintrail.co.uk

Copyright ©Pareto Economics and FINTRAIL. All rights reserved.

