DOI 10.6084/m9.figshare.30278815

Modernizing Compliance: A Synthesis of Identity, Technology, and Regulatory Evolution

5 Counter-Intuitive Truths About Financial Compliance That Everyone Should Know

- by **Slava Solodkiy** (ORCID 0009-0003-8363-4251) github.com/slavasolodkiy/digitalidentity

The landscape of financial compliance is undergoing a fundamental transformation, driven by technological innovation, evolving criminal tactics, and shifting regulatory philosophies. The core purpose of compliance is pivoting from a static, onboarding-focused gatekeeping function to a dynamic, data-driven process of continuous monitoring. The objective is no longer to make a binary judgment of "good" or "bad" but to ensure comprehensive trackability to "follow the money." This shift acknowledges the reality that perfect Know Your Customer (KYC) is unattainable at registration, with evidence suggesting approximately 80% of illicit activity is identified through post-onboarding transaction analysis.

A significant market opportunity is emerging from the rise of "abnormal as the new normal." A growing cohort of high-risk but legitimate clients—including expats, gig economy workers, crypto-related businesses, and individuals in sanctioned or economically unstable nations—is largely excluded by traditional compliance models. This underserved population represents a high-margin, low-competition frontier for innovative financial institutions.

In this new paradigm, Digital Identity is being framed as a new form of value, conceptualized as "the new money" in a burgeoning "reputation economy." However, the practical implementation of decentralized identity faces significant hurdles. These include regulatory reluctance, particularly in the United States, toward "rely on" verification models, and a prevalent technology-first approach, exemplified by Zero-Knowledge (ZK) proofs, which often fails to address real-world client needs and regulatory mandates for accountability.

+ watch on youtu.be/nyl2p6VSs_s, listen on open.spotify.com/episode/olTQISbXsTDVW4oGaTOTIk

To meet these challenges, advanced methodologies from Open Source Intelligence (OSINT) journalism offer a powerful and proven model for the future of Enhanced Due Diligence (EDD) and Anti-Money Laundering (AML). These techniques, honed in high-stakes investigations, provide a template for a more sophisticated and effective approach to compliance. Concurrently, the Banking-as-a-Service (BaaS) model is being forcibly evolved from an ad-hoc arrangement to a "BaaS-first" framework where compliance is deeply integrated, elevating its risk profile to that of correspondent banking and highlighting a growing divergence in regulatory approaches between the U.S., the U.K., and Asia.

1. The Evolving Philosophy of Compliance

The foundational principles of compliance are moving away from an assessment of character or "truth" toward a pragmatic focus on process and traceability. This evolution is rooted in the acknowledgment that financial systems will inevitably be tested by illicit actors and that the most effective defense is a resilient, transparent, and responsive monitoring framework.

From "Truth" to "Trackability"

The central argument is that regulators are not concerned with the absolute "truth" of a customer's nature but with the ability of an institution to trace their financial activities. Compliance is often misperceived as a mechanism to differentiate good people from bad. In reality, its primary function is to establish trackability.
“Regulators aren't focused on the ‘truth’ — what matters to them is that you've considered these types of risks. Compliance is often wrongly seen as a mechanism to differentiate good people from bad. In reality, compliance is about ‘being trackable’ (the ability to trace, to “follow the money”) through a set of dynamic parameters over time.”

The 80/20 Rule of Illicit Activity Detection

The concept of a flawless KYC process at the onboarding stage is considered a myth. Data suggests that initial checks are inherently limited in their effectiveness.
• **Onboarding Limitations:** Only about 20% of fraudulent or malicious actors are identified during the initial registration and Customer Due Diligence (CDD) process.
• **The Power of Monitoring:** The vast majority, approximately 80%, are identified through ongoing transaction monitoring where anomalous patterns emerge.
This reality necessitates a strategic shift: instead of trying to build an impenetrable wall at the front door, institutions must "cast a net" at onboarding. This involves collecting a broad set of parameters that can be used later to detect anomalies and "rewind" to trace connections when suspicious behavior is flagged.

Perpetual KYC (pKYC) and a New Paradigm

The limitations of static, point-in-time checks have given rise to the concept of **continuous or perpetual KYC (pKYC)**. This new paradigm leverages automation, AI, and machine learning to create a dynamic risk profile that evolves with the customer's behavior. An extension of this idea proposes to "simply forget about KYC; let anyone who desires a bank account have one, and use AI/ML to track the bad actors," a concept attributed to David Birch.

The Regulatory View on Errors

Regulators do not expect infallibility. In fact, a perfect record with no mistakes can be perceived as a "red flag," suggesting a lack of depth in scrutiny. When errors or breaches occur, regulators are primarily interested in:
• **Identification:** Who identified the error—the institution, a client, a partner, or the regulator?
• **Response Time:** Was the issue addressed immediately, or was there undue delay?
• **Root Cause:** Was the issue due to a failure in existing controls or an entirely unforeseen risk?

• **Corrective Action:** Are the planned corrective actions specific and well-considered, demonstrating a deep understanding of the issue, or are they generic?

source: https://www.mermaidchart.com/d/b3876675-bc4a-4b56-8f79-9804c7572123

2. "Abnormal is the New Normal": The High-Risk Client Opportunity

Traditional banking's de-risking trend has created a vast and underserved market of clients deemed "abnormal" or "higher-risk." This segment is not inherently illicit but falls outside the rigid comfort zones of legacy compliance systems. This exclusion represents a significant, high-margin business opportunity for specialized and technologically adept financial institutions.

Defining the Underserved Market

The "abnormal" category includes a diverse and growing range of individuals and businesses that are disconnected from the global financial system:

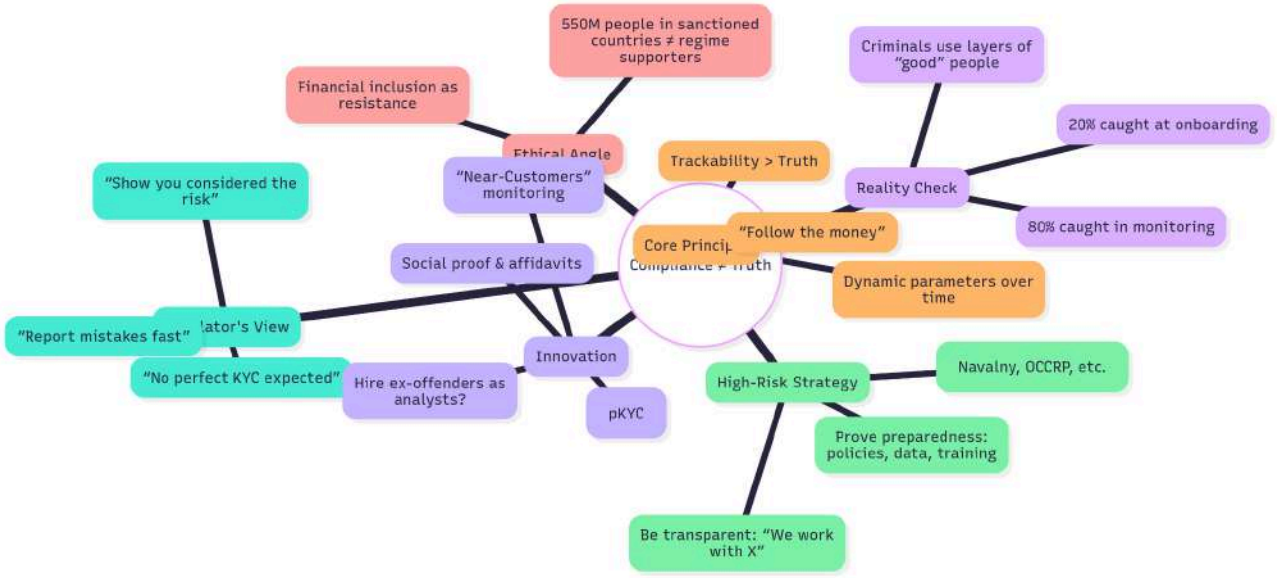
Client Segment	Description
Geographically Disadvantaged	Over 550 million people living in 15 sanctioned countries; 70 million refugees; 56 million expats.
Gig Economy & Digital Natives	Businesses with foreign founders operating remotely from co-working spaces; digital influencers, bloggers, and streamers.
Unbanked/Underbanked	Over 2 billion people globally with no formal banking history.
Stigmatized Industries	Compliant businesses in sectors like cannabis, lawful pornography, and compliant ICOs.

Other High-Risk Profiles	80 million individuals in the U.S. alone with criminal records who face barriers to financial services.

Projects like **nsave**, which secured $4 million in seed funding from investors including Sequoia Capital, exemplify this trend by providing secure offshore Swiss banking services to people in countries with high inflation or unstable financial systems.

A Nuanced Approach to Risk

A modern compliance framework requires moving beyond blanket policies that penalize entire populations. For instance, the oversimplification that all Russian and Belarusian citizens support their governments can lead to the unjust de-banking of dissidents and entrepreneurs. A more nuanced approach, such as the "Scandinavian model" for reintegrating ex-offenders into society, is proposed as a template for the financial sector to serve clients with past convictions, especially for economic crimes.



source: https://www.mermaidchart.com/d/42fe28b7-f17d-44f3-84d8-6470607be2da

3. Digital Identity: The New Money and Reputation Economy

The concept of identity is being reimagined as a core economic asset, forming the basis of a "reputation economy" where trust is established through verifiable digital credentials rather than traditional intermediaries.

Core Concepts

This vision, inspired by thinkers like David Birch, David Graeber, and Milton Friedman, posits that "Identity is the new money." It builds upon several key ideas:

• **Evolution of Money:** Money is not an outgrowth of barter but an evolution of credit—a system for tracking social obligations.

• **Reputation Economy:** Technology can restore a "shared memory" of these obligations, reducing the need for intermediaries and enabling transactions based on "social capital" computed across social graphs.

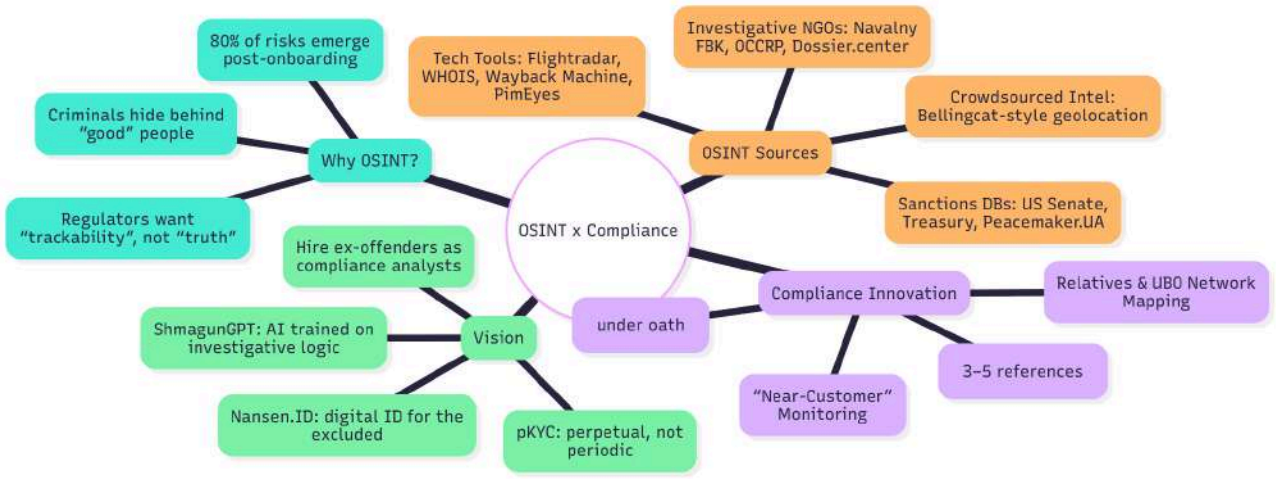
• **Human Capital Contracts:** The idea that individuals can be financed based on their future potential, a concept that aligns with an identity-based economic system.

The Multifaceted Nature of Identity

Digital identity is not a single credential but a complex patchwork of verifiable data points, categorized as follows:
1. **Physical Attributes:** Biometric data like facial recognition, fingerprints, and voice recognition.
2. **Documented Identity:** Official documents such as passports, visas, and certifications.
3. **Social Endorsements:** Vouching from social guarantors, legal professionals, and relatives.
4. **Digital Footprint:** Technical tracers like phone numbers, email addresses, IP addresses, and login credentials.
5. **Personal Affirmation:** Self-declarations made via affidavit-style questions or video verification.

Blockchain and Governance Models

Blockchain technology is proposed as the ideal infrastructure for a decentralized identity system, giving users control over their data and protecting it from the large-scale breaches seen at centralized institutions like Equifax. Different governance models for digital identity are already in practice globally:
• **Estonia's e-Residency:** A pioneering example of a "borderless country" and "government-as-a-service," allowing global entrepreneurs to access its digital infrastructure.
• **China's Social Credit System:** A centralized, state-run system that assigns scores to citizens and companies based on a wide range of behaviors to enforce social norms.



source: https://www.mermaidchart.com/d/f8aadae4-90e6-4c17-87bb-e7a5acf31e26

4. Technological and Methodological Frontiers in Compliance

The future of effective compliance lies in adopting advanced technologies and methodologies that can handle the complexity and scale of modern financial crime. This involves looking beyond traditional compliance tools and learning from adjacent fields like investigative journalism and intelligence.

Open Source Intelligence (OSINT) as a Compliance Model

The techniques used by OSINT investigators represent a paradigm for modern Enhanced Due Diligence (EDD).
• **Proven Efficacy:** Investigative collectives like Bellingcat and journalists such as Christo Grozev (Oscar winner), Olesya Shmagun (Pulitzer winner), and Roman Dobrokhotov have used publicly available data to expose high-level corruption, money laundering, and state-sponsored crimes, including the downing of flight MH17 and the poisoning of Alexey Navalny.
• **Official Adoption:** The CIA has announced a new strategy to expand its use of OSINT and has developed AI technology similar to ChatGPT to automate the analysis of open-source data.
• **Proposed "ShmagunGPT":** A conceptual AI tool for EDD, trained on the investigative methods of experts like Olesya Shmagun to serve as an "automated sidekick for other investigators and compliance officers."

• **OSINT Toolkit:** These methods rely on a wide range of tools for analyzing maps, satellite imagery, photos, commercial registries, vehicle movements, website archives (WaybackMachine), and metadata. Specific software mentioned includes Maigret, Mr.Holmes, Holehe, Ghunt, and DarkGPT.

The "Rely On" Model and ZK Proofs: A Critical View

While technologically sophisticated, solutions like Zero-Knowledge proofs are critiqued as being a "solution looking for a problem that doesn't exist" in the context of current compliance needs.

• **The "Rely On" Debate:** The idea that one financial institution can rely on another's KYC verification is being trialed by the ECB. However, U.S. regulators remain fundamentally opposed, citing the post-9/11 mandate that every institution must be individually accountable for its clients to ensure an unbroken trail for investigators.

• **Critique of ZK Proofs:** The argument is that regulators, banks, and end-users prioritize convenience, speed, and clear accountability over the data non-disclosure that ZK proofs provide. A system based on simple yes/no tokens could obstruct investigations by obscuring the underlying data.

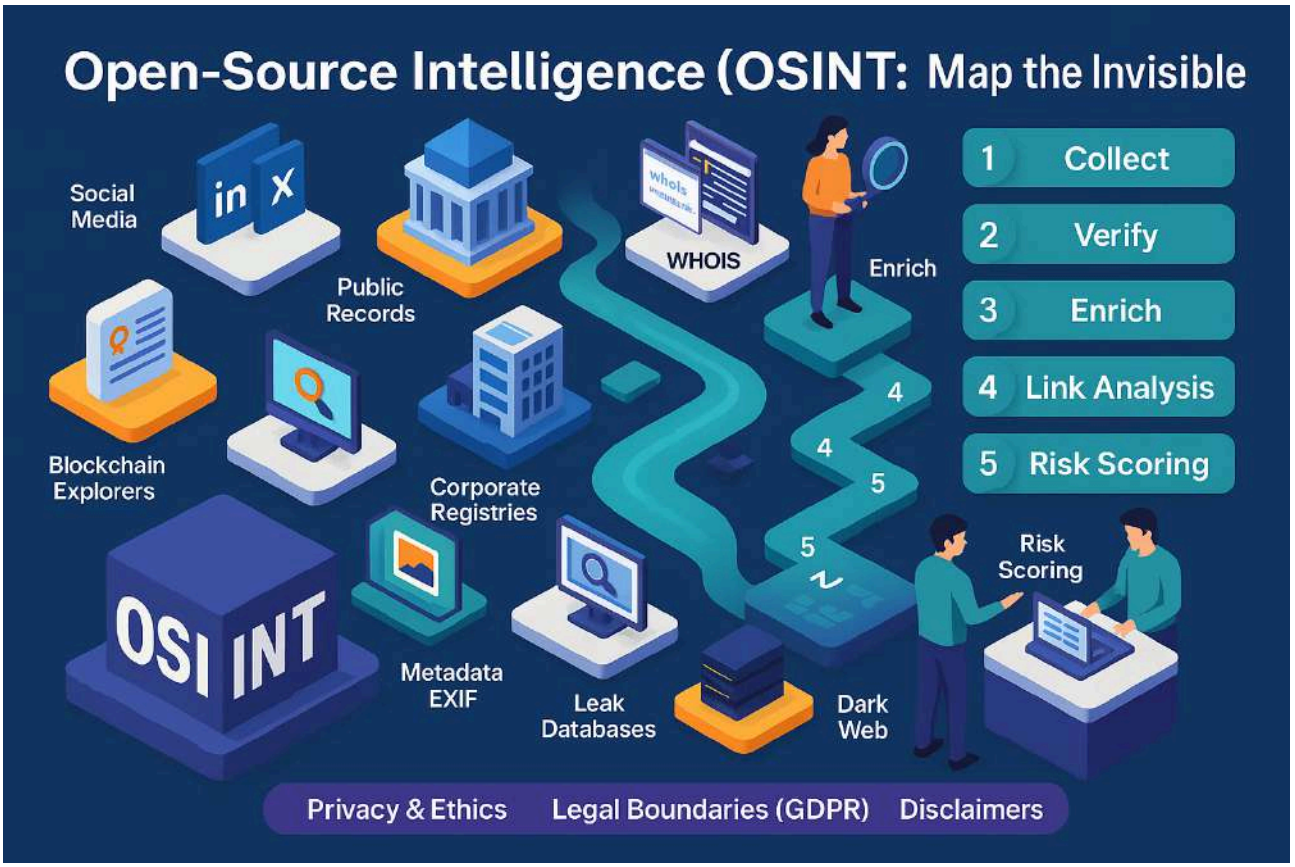
• **A Pragmatic Middle Ground:** A proposed alternative is a system of data "pre-filling." A user's verified information could be used to populate forms at a new institution, but the user must still review and explicitly agree to the data, and the institution must make its own final risk decision.

The Compliance-as-a-Service Model

A proposed product model, A.ID, aim to be the "Stripe or AWS of compliance," specifically tailored for high-risk clients.

• **Architecture:** It is designed as a "Lego-like constructor" that bundles best-in-class third-party verification services into a single, API-driven platform. The focus is on the customer journey, plug-and-play integration, and pay-per-use monetization.

• **Data Philosophy:** It employs a "long-tail" data approach, storing all information to improve the intelligence of its monitoring systems over time. Its architecture uses a "one-to-many" logic, where a single person can have multiple roles (CEO, shareholder, employee) linked to their core identity. It also creates "passive profiles" for counterparties in transactions (senders and recipients), expanding the monitoring network.



https://docs.google.com/document/d/1fMhpRt1eUI7uqGQOcymSH_JbEsfDkkD4j0m1qyKLCqM/edit?usp=sharing

5. The Restructuring of Banking Models: BaaS and Correspondent Banking

The Banking-as-a-Service sector is undergoing a period of intense regulatory scrutiny, particularly in the U.S., forcing a fundamental restructuring of the model.

The BaaS Crisis and Evolution

The era of the ad-hoc BaaS partnership is over. A series of enforcement actions has signaled a shift to a **"BaaS-first"** model, where compliance is not an afterthought but the central component of the business architecture.

• **BaaS as Correspondent Banking:** U.S. regulators now explicitly treat BaaS relationships with the same level of risk and scrutiny as correspondent banking.

• **The Core Mandate:** The primary regulatory demand is for sponsor banks to embed their own compliance engines and risk management frameworks directly into their fintech partners' operations. This requires real-time **KYCC (Know Your Customer's Customer)** capabilities, moving far beyond retroactive paper checks during audits.

International Regulatory Divergence

A notable gap is emerging in the regulatory handling of these new models across different jurisdictions.

• **United Kingdom:** The U.K. is seen as more forward-thinking, having granted a full banking license to **Griffin Bank**, an institution built on a BaaS-first, compliance-centric model. This signals an understanding that modern banking can be transactional and infrastructure-focused.

• **United States:** The U.S. regulatory environment is described as more fragmented and reactive, hampered by competition between different agencies and lobbying from traditional regional banks. This has created an atmosphere of uncertainty that stifles innovation.

• **China:** China is moving ahead with its Central Bank Digital Currency (CBDC) project, indicating a different strategic priority.

6. Five Counter-Intuitive Truths About Financial Compliance That Everyone Should Know

We've all been there: mired in the digital paperwork for a new bank account or mobile plan, feeling the familiar frustration of a process that seems both repetitive and invasive. This friction is more than just an inconvenience; it’s a symptom of a global financial compliance system that most of us fundamentally misunderstand—a system whose very purpose is undergoing a radical transformation.

We see walls designed to keep people out, but a new architecture of trust is being built. This evolution is redefining the nature of identity, enabling greater financial inclusion, and shifting the focus from rigid gatekeeping to intelligent, dynamic monitoring. This article will pull back the curtain on the world of Know-Your-Customer (KYC) and digital identity to reveal five surprising truths that challenge our common assumptions. These aren't just interesting facts; they are the pillars of a smarter, more inclusive financial future.

6.1. Compliance Isn't About Judging 'Good' vs. 'Bad' People

The most common misconception about financial compliance is that it's a moral test—a system designed to separate trustworthy individuals from potential criminals. When we're asked for extensive documentation, it feels like we're being judged. But the core objective for regulators is not to determine the absolute "truth" about an individual's character.

The actual goal is to ensure that financial activities are **traceable**. To put it bluntly, compliance isn’t about preventing every bad act before it happens; human behavior is too complex for that. A more powerful analogy is this: compliance isn’t about ‘preventing 9/11,’ but when it happens, ‘to quickly find who is involved.’ This perspective shifts the entire paradigm. The system is not a moral gatekeeper

designed to "follow the person," but a forensic tool designed to "follow the money." Its primary function is not to prevent all illicit activity at the door, but to enable swift, decisive investigation when it occurs. "Regulators aren't focused on the “truth” — what matters to them is that you’ve considered these types of risks. Compliance is often wrongly seen as a mechanism to differentiate good people from bad. In reality, compliance is about “being trackable” (the ability to trace, to “follow the money”) through a set of dynamic parameters over time."

6.2. Onboarding Is Just the Tip of the Iceberg: 80% of Crime Is Caught Later

We tend to think that a slick, rigorous sign-up process is a fortress against financial crime. In reality, the initial onboarding stage is just the first line of defense, and it's far from the most effective one. A staggering 80% of fraudulent activity is not caught at sign-up; it's identified later through ongoing transaction monitoring.
Why? Because the real slick criminals layer their operations with legitimate transactions, often using innocent people as shields and intermediaries. No onboarding system, no matter how sophisticated, can red-flag these operations from the outset. The true purpose of the initial KYC process, therefore, is to "cast a net." It’s about collecting enough data at the start so that anomalies in behavior—unusual transaction patterns or connections—can be detected later, allowing investigators to quickly rewind the tape and pinpoint the bad actors and their accomplices.
"it’s crucial to grasp that the slickest KYC process at onboarding won’t shield you from fraud and scammers: only 20% get caught at the get-go, while the other 80% are nabbed based on their transactions later on. To catch these guys later, you need to "cast a net" at onboarding so that any anomalies in behavior can be spotted more swiftly, allowing a quick rewind to pinpoint accomplices."

6.3. The World's Best Compliance Experts Aren't in Banking—They're Investigative Journalists

When we think of compliance experts, we picture people in suits analyzing data in corporate offices. But the real innovators in tracking illicit financial flows aren't in banking at all—they are investigative journalists and Open Source Intelligence (OSINT) investigators.
Organizations like Bellingcat and figures such as Christo Grozev and Pulitzer-winner Olesya Shmagun have pioneered methods for untangling the world's most complex corruption and money laundering schemes. Their superpower isn't access to secret banking ledgers; it's the mastery of publicly available data. Take Bellingcat’s investigation into the downing of Malaysia Airlines flight MH17. They tracked the missile launcher's movement from Russia to Ukraine by piecing together evidence from eyewitness photos, satellite images, and social media videos. By analyzing data as varied as mobile operators' billing records, passenger lists, and leaked commercial databases, these investigators connect dots that traditional systems miss. Their work is a masterclass in holding power to account, and the financial industry has everything to learn from their fresh, unconventional insights.
"And regarding #compliance, #KYC, and #AML - I would recommend regulators, banks, and fintechs to learn from them (as the #CIA does), rather than from conferences and office research by major consulting firms."

6.4. The Future Is "Perpetual KYC": Let Everyone In and Track the Bad Actors

The current compliance model often functions as a blunt instrument, inadvertently excluding millions of legitimate customers who don't fit a standard profile. The system flags huge, growing populations as "abnormal" and locks them out. This includes **expats, gig economy workers, refugees, the unbanked, digital influencers,** and even residents of sanctioned countries who oppose their regimes.
A new, more effective paradigm is emerging: perpetual KYC (pKYC). This represents a radical shift from gatekeeper to watchdog. Instead of a rigid, one-time check at the door, pKYC advocates for simplifying onboarding to let almost anyone in. The real work begins afterward, using sophisticated AI and machine learning (AI/ML) to monitor transactions and behavior in real-time. This approach focuses resources where they matter most—tracking actual bad actors—rather than wasting them on excluding

vast segments of the global population. It's a more inclusive, efficient, and ultimately more secure model for the modern economy.

“simply forget about KYC; let anyone who desires a bank account have one, and use AI/ML to track the bad actors,” said David Birch, and he was correct. Soups from Sardine.ai made a similar comment to me recently about working with high-risk clients — “KYC is just the simplest part, the real interest starts afterward.”

6.5. Your Digital Identity Is Becoming More Valuable Than Your Credit Score

For decades, our trustworthiness has been distilled into a single number: our credit score. But in our hyper-connected world, this narrow metric is becoming obsolete. We are moving toward a "reputation economy," where trust is derived not from credit history but from our "social capital."

This isn't just a futuristic trend; it's a return to a more fundamental way of establishing trust. As money historian Jack Weatherford noted, technology is returning us to a "neolithic world economy" that operated on a "shared memory of mutual cross-obligations." Before formal money, trust within a community was based on reputation and relationships. Today, technology is recreating that shared memory on a global scale. Your social capital is the sum of your entire digital footprint—your social graph, transaction history, professional networks, and online activities. In this new paradigm, your holistic digital identity becomes the foundation for all economic exchange, a far richer and more accurate measure of trust than any single score.

“This "social identity" is the basis for a reputation economy, an economy based on trust. It will be reputation rather than regulation that will animate trust in economic exchange, and that social graph, the network of our social identities, will be the nexus of commerce, administration and interaction.”

Conclusion: A Smarter, More Inclusive Future

These five truths paint a clear picture of the future. We are moving away from a rigid, exclusionary compliance system toward one that is dynamic, data-rich, and intelligent. The goal is no longer to build walls but to build traceable networks; not to judge character but to understand behavior.

This isn't a minor tweak—it's a complete reimagining of trust for the digital age. For the end user, this future feels seamless. It’s a world where your identity is portable and continuous, where opening an account is simple because your reputation precedes you, and where the global financial system is both more accessible and more secure. We are building a world where trust is no longer a snapshot in time, but the living, breathing sum of our digital lives.

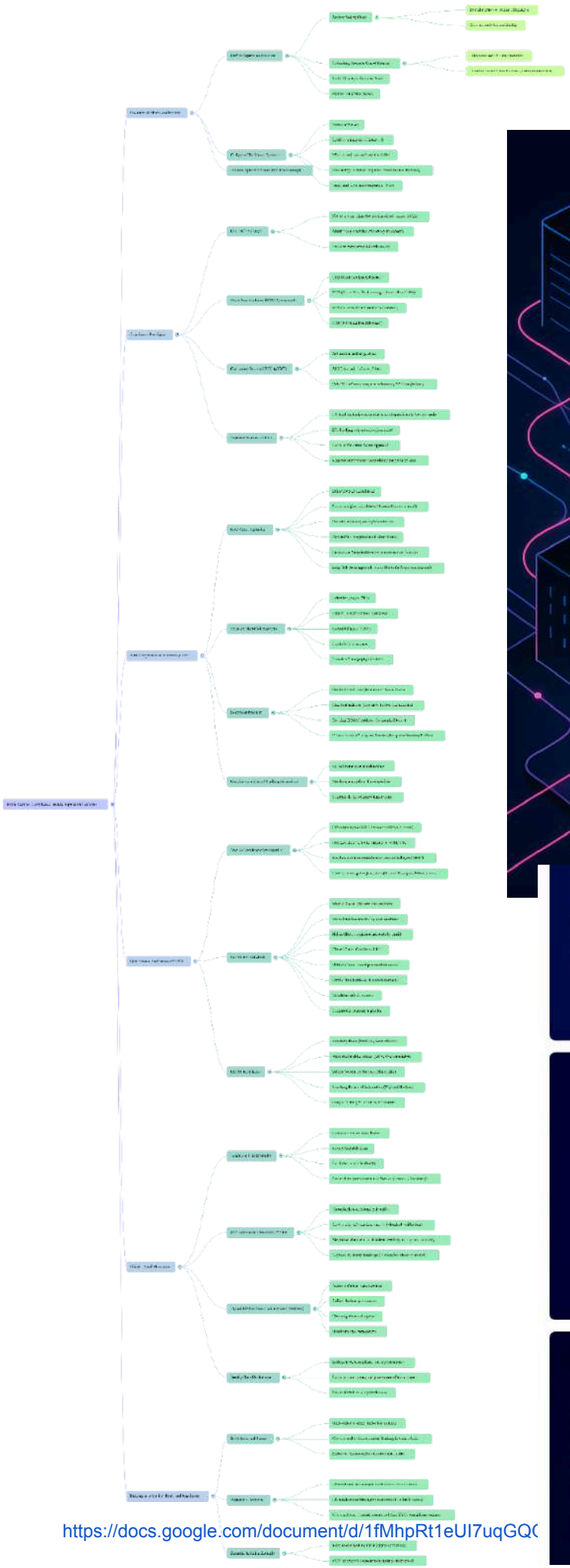
Sources [15]

1. https://notebooklm.google.com/notebook/9692c267-10ae-4724-9a45-f2a168e039c5?authuser=4
2. High-Risk Compliance for BaaS and Correspondent Banks https://www.linkedin.com/pulse/high-risk-compliance-baas-correspondent-banks-vladislav-solodkiy-4eotc/
3. Arival attains the (SOC1 and) SOC 2 compliance report https://medium.com/arivalbank/arival-attains-the-soc-2-compliance-report-22c39956a18b
4. How we created the coolest compliance ever https://medium.com/arivalbank/compliance-is-sexy-and-arival-knows-it-3d7094f53131
5. Digital Identity is the new money https://www.slideshare.net/slideshow/digital-identity-is-the-new-money/100705902
6. Compliance-as-a-Service solutions https://www.slideshare.net/slideshow/arrival-of-aid-complianceasaservice-solution/174265982
7. Compliance Demystified: A Beginner’s Guide https://medium.com/@slavasolodkiy_67243/compliance-demystified-a-beginners-guide-d41342fdc056
8. The Regulator doesn’t care about the ‘Truth’ https://medium.com/@slavasolodkiy_67243/the-regulator-doesnt-care-about-the-truth-there-is-no-perfect-kyc-16385ebbf14d
9. OSINT: They Are Much Better Than Your Chief Compliance Officer https://www.linkedin.com/pulse/much-better-thank-your-chief-compliance-officer-vladislav-solodkiy-a2zgc/
10. From Dissident to Detective https://medium.com/@slavasolodkiy_67243/from-dissident-to-detective-on-the-way-to-shmagungpt-6bcf05c3fbba
11. ZK Proofs: Chasing Problems That Don't Exist? https://www.linkedin.com/pulse/zk-proofs-chasing-problems-dont-exist-vladislav-solodkiy-wqble/
12. How could World ID be better? Or at least useful https://www.linkedin.com/pulse/how-could-world-id-better-least-useful-vladislav-solodkiy-ri4me/
13. Correspondent banking market overview (and KYCC-problem) https://www.slideshare.net/slideshow/correspondent-banking-market-overview/262636406
14. Following the Money: A Journey Through Shadow Banking and Power Games (Compliance Cowboys: The High-Risk, High-Reward World of ‘Ozark’) (ASIN B0DM9NL54Y, ISBN 979-8345524121, DOI 10.6084/m9.figshare.30228340) https://figshare.com/articles/book/Following_the_Money_A_Journey_Through_Shadow_Banking_and_Power_Games_Compliance_Cowboys_The_High-Risk_High-Reward_World_of_Ozark_/30228340?file=58332787
15. Unveiling the Underworld of Global Finance (DOI 10.6084/m9.figshare.30228382) https://figshare.com/articles/preprint/Unveiling_the_Underworld_of_Global_Finance/30228382?file=5833287

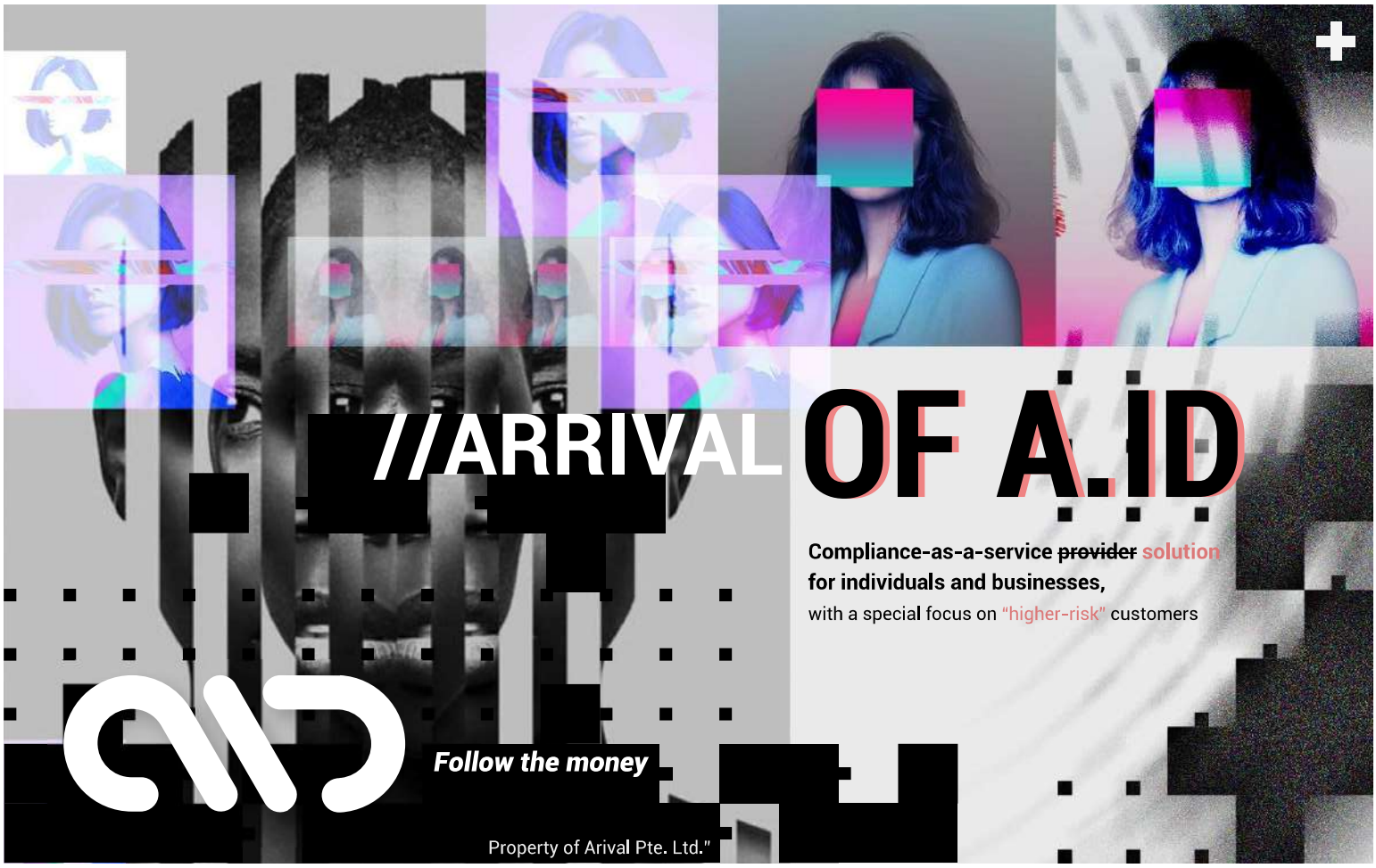
All illustrations by

https://www.behance.net/gallery/235857165/Isometric-Infographic-Illustrations-For-My-Articles

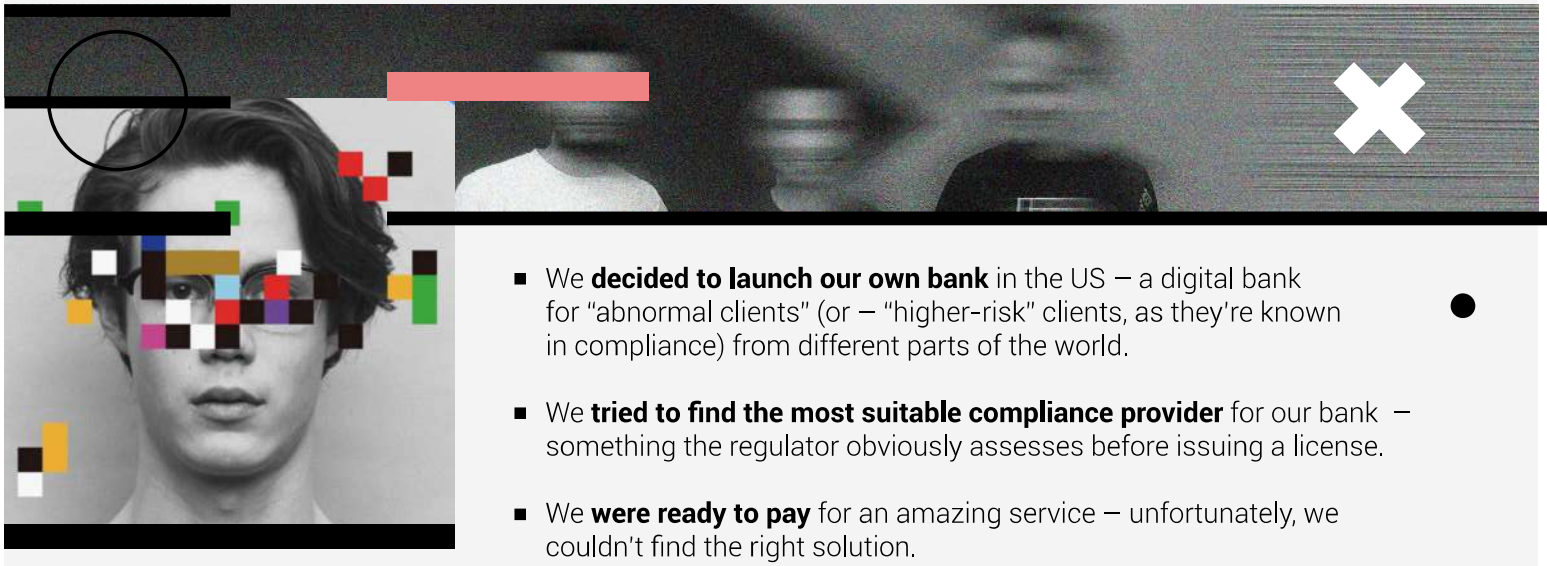
https://docs.google.com/document/d/1fMhpRt1eUI7uqGQOcymSH_JbEsfDkkD4j0m1qyKLCqM/edit?usp=sharing



https://docs.google.com/document/d/1fMhpRt1eUI7uqGQ(



How did we start? **What problem are we solving?**



- We **decided to launch our own bank** in the US – a digital bank for "abnormal clients" (or – "higher-risk" clients, as they're known in compliance) from different parts of the world.
- We **tried to find the most suitable compliance provider** for our bank – something the regulator obviously assesses before issuing a license.
- We **were ready to pay** for an amazing service – unfortunately, we couldn't find the right solution.
- We have **met many (!) other banks** and fintechs (both old & new), who have cried out the same problem.
- We then asked ourselves: **what if somebody like Stripe or AWS were to exist, but for compliance?**

COMPETITIVE ANALYSIS:

they have "functionality" – yet

- Too many compliance providers on the market are in search of deep pockets. Not enough are focusing on your problems. They're holding your hand while sharing some basic suggestions, but that isn't enough.
- Everybody is **just one piece of the puzzle:**
  - One is **focused on KYC,** the other on KYB
  - One **focused on onboarding** and CDD, the other on AML monitoring and ongoing compliance
  - One **focused on ID verification,** the other on background checks and blacklists
  - One **focused on EU** markets, the other on the US, etc
  - And nobody is paying **attention to the end-users**...i.e. you (as a user of a bank or fintech). I doubt anybody will align their compliance experience based on your feelings or what is convenient for you.

Follow the money

COMPETITIVE ANALYSIS:

we need "problem solving"

- **Integrations are difficult** and quite expensive:
  - **No plug & play:** you'll need to go through the pecking order...many calls, sign contracts, deliberate with their product team, and ultimately have your own tech team in place
  - **No pay-per-use:** expect to pay deposits and to commit to a minimum volume (i.e. verifications)
- **Nobody is focusing on higher-risk** clients and "abnormal" use cases. Everybody is tailored for traditional clients with common requirements.
- Some have unicorn valuation and boast having Uber and Airbnb amongst their clientele, **but not a single bank in their pipeline.** As you can imagine, having a bank on board is the market's "sky high" achievement considering they're respected by regulators more than anybody else.

This material and presentation may not be altered, modified, or otherwise used elsewhere without the written consent of Arival Pte. Ltd.

WHY is the focus on higher-risk clients so important?

Simply put, because today **abnormal is the new normal:**

- **More and more segments are falling into the abnormal category;** in other words, these are customers disconnected the financial system and excluded from modern banking services:

Digital influencers: bloggers, streamers, artists

70m+ **refugees**

The 2b+ people currently **unbanked** (poor, minimal education, with no history of bank accounts)

150m+ **homeless** people (nearly 1.6 billion, more than 20 percent of the world's population, may lack adequate housing)

56m+ **expats** across the world

Cannabis industry

Lawful Pornography Industry

Compliant ICO

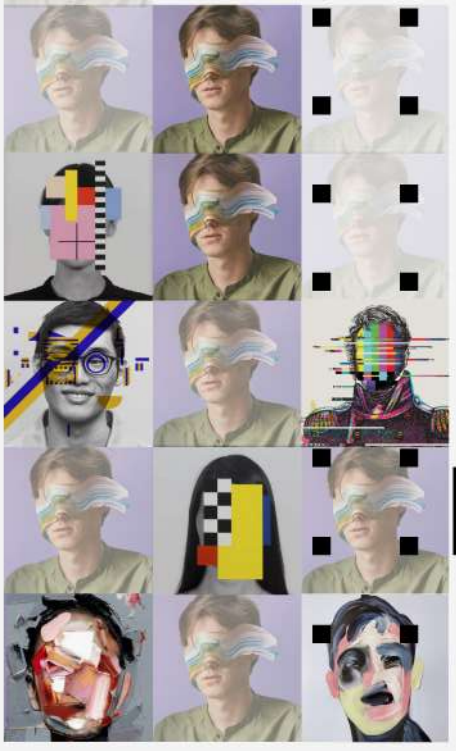
40k+ thousand businesses from around the world registered with Estonia's **e-Residency** program

Businesses with **foreign** founders + doing business remotely or internationally from co-working spaces (this is a nightmare for traditional compliance players that view them without physical and operational presence in their respective country)

This list will only grow. It seems like the **abnormal segment will soon be bigger than any traditional customer segment on the market.**

- If you work with higher-risk clients – you can serve low-risk clients as well. Not vice versa.

What does a focus on high-risky clients means for us?



01 Easier to differentiate from competitors

02 Higher margin = high profit and there is no need for "price wars"

03 Empty niche = zero marketing costs for customer acquisition

+

Our product: → We are like the Stripe or AWS of compliance

We are not the newest, coolest, tech creators, or a team of 007 style spies & investigators, or the owners of the most expansive database known to man – we are like Stripe or AWS, but for compliance. Our customer value proposition consists of five main elements:

01

We "own" only one thing inside our "product" – the customer journey: the convenience of compliance implementation, integration and usage for any bank or fintech

02

Bundling - for each step (or 'container'), we aggregate the best providers (the more the better if they fulfill the entire spectrum of requirements, procedures, etc)

03

Plug & play integration – no need for calls, meetings, presentations, MOUs, LOIs, NDAs, contracts, a tech team in place, web servers, weeks or months, just our easy API (or short link):

04

Pay-per-use monetization – no need for deposits, minimum volume, and wholesale prices for retail usage

05

Long-tale approach – we always store all the data: to guarantee the lowest prices for you, to make our compliance monitoring and decisions better and more intelligent, and to make the registration process for your end users more convenient and safe.

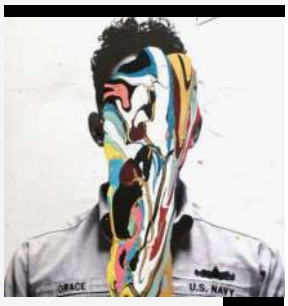
01 02 03 04 05

Our product: 01 → We "own" only one thing inside our "product" – customer journey:

How do we create convenience from compliance implementation, integration and usage for banks and fintechs?

- As customers, we immediately understood that the players on the market today are simply providers (databases, technologies, etc) – and nobody is trying to solve the customer's problem as a **one-stop-shop solution**
- We've analyzed many, many customers' journeys across the world: via traditional and digital banks, fintechs, compliance providers = and we built our own vision of **the best customer journey**

We designed the logic ourselves, and on each step or part, we add one or several custom providers, focused on the exact process or type of data.



Our product: 02 → Bundling

The five parts of our product:

01 **Lego-like constructor** – enabling you to build your own onboarding forms to work with individuals or businesses, setup risk profiles, yellow and red flags, #hashtags for transaction monitoring, etc; customize colors and logos;

02 **API** – download a few lines of code and integrate our solution inside your website or app, or just use short links without integration;

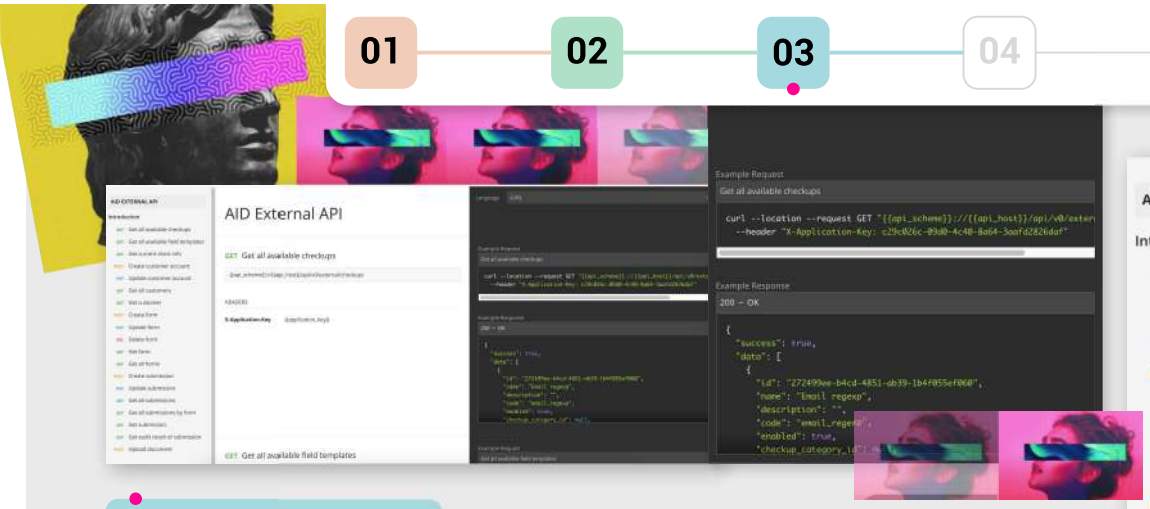
03 **oAuth** – a secured login & password form for your end-users; register; share existing data with new banks or fintechs;

04 **Compliance officer dashboard** – an overview of all users (accepted, rejected, in process), the ability to analyze yellow and red flags, ask questions regarding onboarding forms or transactions, radar placement, add comments, edit or create new #hashtags, create and send reports;

05 **End-user interface (active and passive profiles)** – add, edit or delete data & docs, monitor who-when-why-how used certain data & docs, request to delete data & registrations, create and manage claims;

For each step (or 'container'), we aggregate the best providers (the more the better):

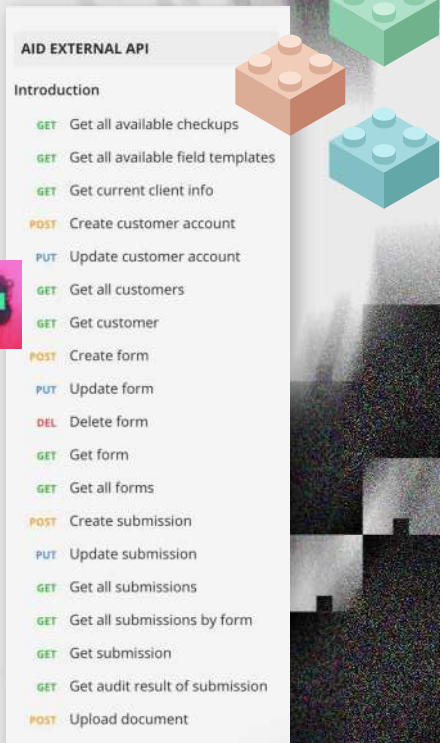
- Sometimes it is only one provider for some "container", or sometimes almost 10
- Sometimes (not often) there is no provider – and we'll do it by ourselves

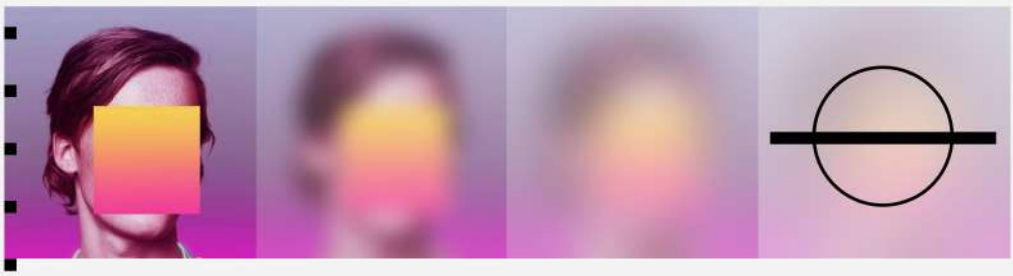


Our product: 03 → Plug & play integration

No need for calls, meetings, presentations, MOUs, LOIs, NDAs, contracts, a tech team in place, web servers, weeks or months, just our easy API (or short link):

- Build your customer journey and any other parameters by yourself – like LEGO bricks, if you can create a Facebook page, then you have enough skills to build your own compliance solution, using our templates;
- Just copy-paste several lines of code from our API store;
- Customize interfaces by yourself: logos, wording, colors, etc;
- Don't want to use an API? Just copy the short link and send it to your end users via email, Facebook, WhatsApp, Instagram, etc.

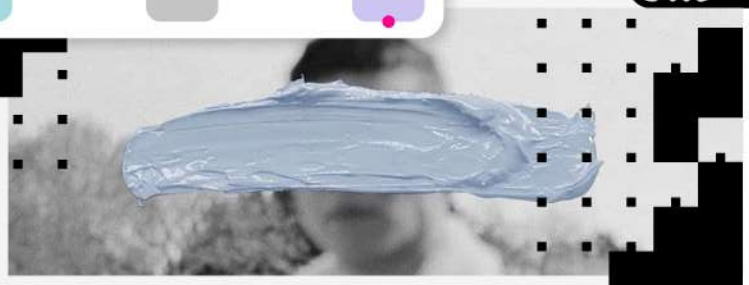




Our product: 03 → Pay-per-use monetization

No need for deposits, minimum volume, etc, and wholesale prices for retail usage, and "long-tale" data amortization:

- **Why are our prices so low?** We commit to a high amount of verifications with each vendor to have the lowest possible prices, pay the deposits ourselves, guarantee a minimum amount of verifications, etc = and then sell you the same wholesale prices, but one-by-one without any commitments and deposits;
- Our margin for each bundle is very transparent: **our incurred expenses for each verification + 4pp** (this is our profit, which is a very, very low margin-per-verification);
- Why is our margin-per-verification sooooo low? Because we don't think about each verification – we think about customers (you) and their end users (you too). We store all the data after each verification on our side, and we expect that we will have approximately 3-5 verifications per user sooner or later (and our margin will ultimately be very high – meaning we can ~~pay more dividends for our shareholders~~ develop more and more products and useful features for you and your end users).



Our product: 05 → Long-tale approach

We always store all data: to guarantee the lowest prices for you, to make our compliance monitoring and decisions better and more intelligent, and to make the registration process for your end users more convenient and safe = win-win-win situation

Why is storing the data with us a good idea for you? We know you don't like this idea, and to be honest, we feel you, BUT:

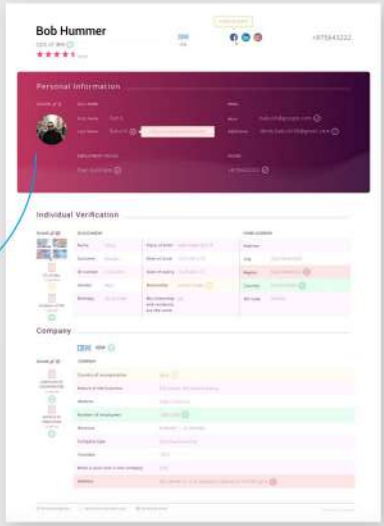
- This is why our **prices are so low for you**
- More importantly - **it increases the quality of compliance 20x:**

  Only 5% of money laundering cases could be "caught" during the onboarding process (because criminals are not stupid and always improve their tactics)

  The only one way to combat such a problem is to know and track much more: asking more questions, collecting more data (to compare and analyze), connecting the data from onboarding with further ongoing compliance activities and transactions (not to mention, **analyzing external senders and receivers as "passive" users as well**); essentially, understanding the financial activity of end users...where and when, and with who

- Super convenient for your end users

Why are we the first ones that care about your **end users?**



- Because **you care about them** (at least we hope so)
- **Today,** at any given time, they can be successfully onboarded with your service
- **Tomorrow,** they will have value (starting from 2+ registrations):

  + the same login & password for each new registration = **easy to remember;**

  + No **wasting time and nerves:** no more redundant onboarding and registering over and over again = with permission, we can securely share the end users' "stamp of approval" with new banks or fintech services of choice;

  + **control and manage their private data:** add, edit, delete information and docs, track who-when-why -where requested and used their data, request to delete, create and manage claims.

Follow the money

Converting fear **to convenience** (with good rates!):

+ Yes, we collect a lot of data of your end users – we understand this is super sensitive data, and we need to be extremely cautious, responsible and transparent with you

+ We share information only with your permission with a transparent description of who, what and why + any other requests from your side;

+ You will always see and control: who viewed the data, when, where, why, how they used your information, and for which reasons,

+ you can request to delete the data, create a dispute or make a claim

Plus, you can use **our app for 2Auth-verification** for your future transactions too! (Later on, you'll have the ability to become a "wallet" to store & share all your verified documents and other data.)

Why only banks and fintechs?

Compliance is everywhere – we plan to scale for:

- **The sharing economy** – check out how much crime involves Uber drivers or people via Airbnb because "they only verified just the identity" (rather than background checks, cross-checking social connections, etc)
- **Social media and messengers** – fake news, fake accounts
- **Dating services**
- **Insurtech and Medtech** – add your health data from different providers to improve the understanding of your health (and to decrease rates for insurance and medical bills);
- **Travel** – automation of visa applications, frequent tourist procedures, check-ins at airports and crossing the border, etc
- From KYC and KYB to **Know-Your-Employee and Know-Your-Partner**

Compliance is coming: companies like Amazon and eBay have already encountered "compliance issues" (trade money laundering) – in 5 years, mom-and-pop shops will be obligated to have compliance officers and policies.

Why should you trust us?
How do we know our approach works?:

01 **We've tested it on our own case** with the US regulator – our bank became the first client:

- **A** The US is the hardest jurisdiction in terms of banking regulation and correspondent banking relationships;
- **B** We've applied for a banking license to work with higher-risk segments;
- **C** We've worked with Promontory Group (one of the most respected compliance firms in the world based in Washington DC) and DLA Piper (international legal firm), and analyzed many vendors and approaches;
- **D** Other vendors (on their own) weren't sufficient enough to grant our license, but finally we received our license with our own solution. Ok, ***how many vendors on the market received any license by themselves for themselves?***

02 Our bank works a lot with **other fintechs** – we are approached by them to integrate our solution for their internal usage in order to improve their compliance;

03 We've been **approached by a bunch of other banks** (feel free to request direct feedback after NDA) from different jurisdictions who wish to improve their compliance without additional expenses and headaches.

Compliance is sexy, and A.ID knows it

How we created the coolest compliance ever

How do you check your clients? How do you onboard them? How do you make sure your bank or fintech startup won't be used for money laundering and other criminal activities?

When you acquire a bank, apply for a banking license or launch a new fintech startup – you will be on the radar of regulators.

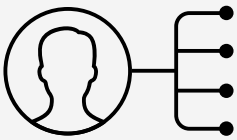
In case **your clients fall under the 'higher-risk' category**, you go to bed thinking about compliance and wake up to the very same thought. Regulators had other plans for you – "...no way, you have to be a 6 on a five-point scale if you want to work with these type of clients. Surprise us."

Compliance it is not only KYC – it is consists of many things in complex:

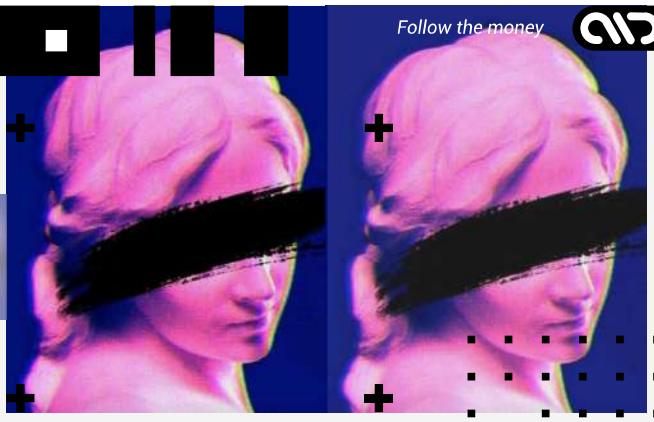
- **CDD**, customer due diligence (KYC & KYB);
- **EDD**, enhanced due diligence;
- **Ongoing compliance:** AML and transaction monitoring.

Other blocks aren't visible to clients and are related to bank's internal processes:

- Segmentation of clients and Risk profiling;
- Internal controls, Internal and External Audit;
- Client offboarding;
- Monitoring & Reporting;
- Education & Assessment.

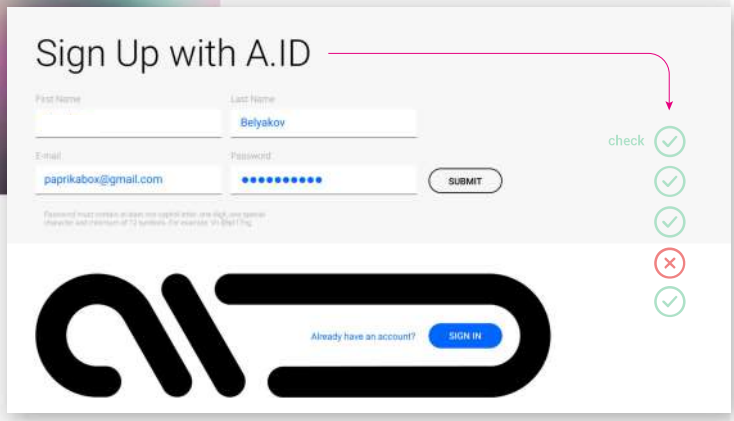


ONE-TO-MANY



Architecture of a user account is created according to the **'personality + set of roles'** logic.

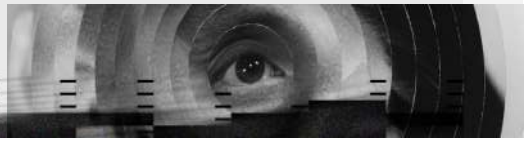
- ***Example:*** Let's say, you are an owner or an employee at several companies: you will have a basic individual account with your name, with your roles 'CEO of company №1', 'Employee of company №2' or 'shareholder of company №3' tied to it.
- The system constantly checks the entire database for similar accounts in order to avoid double accounts or fraud.
- Most banks create a new entity for each type of relationship, which resembles schizophrenia and gets in the way of compliance, which will be more efficient if you possess more data on a client in a single account.
- When someone signs up or logs into their bank account – it is never a company, rather a specific person, and we always need to know who it is to trust each other.



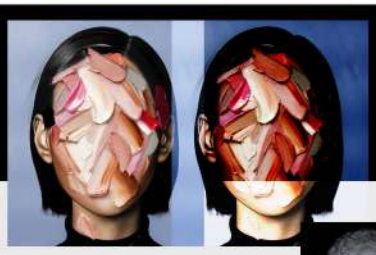
oAuth: IP-address and MAC-address checking

When you sign up and later log in to the system each time, the IP-address and MAC-address of your device are scanned automatically to understand the geography of your internet access and the type of device you log in from:

- Whether a user uses a single device for log in or suddenly a new device comes up, and how often they change;
- Whether a user logs in from an unexpected country (including countries under sanctions) compared to his previous behavior;
- Time zone is being defined and 'traditional' log in hours are filled in automatically.
- The solution is created in a way that if an unusual situation happens, you are not blocked, but asked questions. If suspicion arises that somebody answers the questions for you, a video call will be initiated.
- You can choose the settings yourself: whether you add your IP- and MAC-address to the 'trusted' list or it was a one-time log in



CDD
(Customer Due Diligence)



KYC (Know You Customer)

- Mobile number and e-mail verification
- Passport and ID verification
- Confirmation of residence address
- Bank card verification
- Add your social network accounts (Facebook, LinkedIn, etc)
- Fill in type of employment and average income level
- Record a short video of yourself
- E-signature
- Background checks of the person

KYB (Know You Business)

- The company data: name, name in the system, legal name, country, date and number of registration, industry or several industries, website, LinkedIn, Facebook or Github page, Address, number of employees in your company;
- Estimated turnover and countries where you plan to receive/send money most frequently
- Ownership structure information: management and shareholders
- Background checks of the company, shareholders and management

KYC (Know Your Customer)

Follow the money

Mobile number and e-mail verification – you receive a code for verification

- we assume that you might have several phone numbers and e-mails
- we check what provider and country it belongs to (to match your country of citizenship, residence or internet access)
- we also aggregate meta data based on how frequently this provider is used for fraud

Confirmation of residence address

- you can have multiple addresses in different countries
- you can confirm your addresses traditionally – by providing utility bills or bank account statements
- as well as asking us to send you a physical letter with a unique code (you can pick it up upon the presentation of a passport only)
- all addresses are checked with Google Maps and other online maps instantly, and are checked for public information about these places (what else is present there, the type of building, etc.)

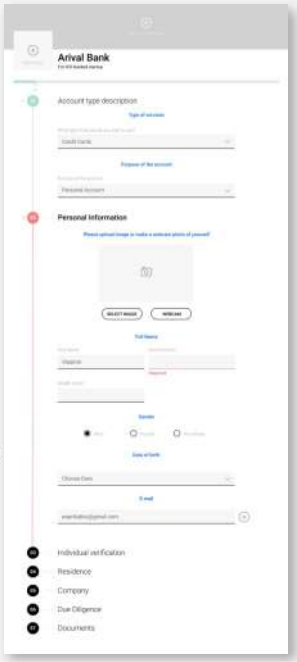
Passport and ID verification

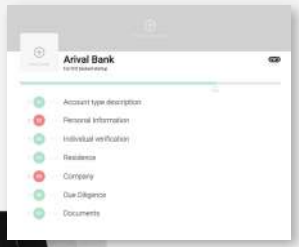
- we provide you with an opportunity to upload more than one document: the world becomes more and more 'horizontal', people constantly move, and it is simply stupid to tie a person to one single country
- we automatically take a note on the expiration date of each document – the system will remind you and itself to renew your document
- we check documents for any alterations or other intervention
- we check databases for any criminal records, sanction lists, blacklists, etc.
- we check whether the country of internet access matches place of your citizenship or residence

E-signature

- your approval for A.ID to collect, store and analyze this information (until you change your mind and ask us to delete it),
- pass it to other banks and other partner fintech services (only with your additional future consent and permission)
- we compare it with your signature on your ID

KYC (Know Your Customer)



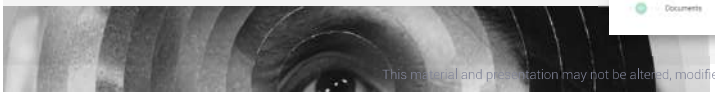


Bank card verification

- We believe it's weird if you have no bank card at all – but it is reasonable if you are underage, or from an unbanked country, or a refugee, etc.
- You fill in the card data (we don't store it)
- We check the type (gift-cards don't work, classic debit or credit cards are welcome)
- Whether it is active or not (we charge a small sum and return it instantly
- Remember its expiration date (to ask you to update this information), and attentively examine the card's issuing bank
- The same works for bank account statements. We store them separately and analyze which banks have already verified you before us (if any), their country and reputation

Recording a short video of yourself

- As we don't see each other face to face, we need to know that your data wasn't stolen by a malicious user.
- We compare your video with photos from documents (and social networks, including YouTube)



Add your social network accounts (Facebook, LinkedIn, etc)

- we will assume it suspicious if there is zero information about you on the internet – but it's possible.
- knowledge of your social network account (only if you decide to share it with us – you can choose to not share the information in each step)
- we do a comparison of your name and last name, e-mail and profile picture with the ones you provided
- At the same time, your decision to share your social connections (friends, colleagues, family) will be taken positively for ongoing compliance and AML (it allows us to build trust on your senders and receivers).

Fill in type of employment and average income level

- You can check relevant boxes if you wish to tell us more about you (or not).
- The higher transaction amounts you expect with your account, the more interested we become in who you are and what you do for living (I think you understand why, don't you?).

What else can we ask end users via A.ID?

- Relatives of the user (important for PEPs)
- Biometric data: facial recognition, voice recognition, fingerprint recognition (important for refugees and homeless people)

KYB (Know Your Business)

Who exactly represents the company – now and in the future

- When someone signs up or logs into their bank account – it is never a company who does this, but a specific person, and we always need to know who it is in order to establish trust.
- You can add your role (which you can change in the future): your relation to the company opening an account in the bank. You need to specify your position in the company (shareholder, director, employee or outsourced accountant) and confirm that you are authorized to open the account for it.

Provide ownership structure information

- What percentage of shares belongs to whom - you just state the percent, person's name or holding company name, and contact e-mail
- Beneficiaries will have to pass verification themselves – we will send them a notification and link.
- Also, we will need your CEO's (and other top managers) contact e-mail.
- Any company is a group of people (KYCs), including its ultimate beneficiaries, and of course those working and managing it.
- In terms of beneficial ownership compliance rules, most regulators require companies to disclose information about any shareholders with a 25% stake or higher. In our case for higher-risk clients, we'll go from 10% and higher.

You will fill in the company data:

- Name, name in the system, legal name, country, date and number of registration.
- You choose what industry or several industries it belongs to.
- Website, LinkedIn, Facebook or Github page – if you have it.
- Address: one or many.
- We check if there has been any adverse media or criminal information about your company across different data basses, blacklists and sanction lists.
- You fill in an approximate number of employees in your company, estimated turnover and countries where you plan to receive/send money to most frequently.

KYB (Know Your Business)

Provide ownership structure information

- What percentage of shares belongs to whom - you just state the percent, person's name or holding company name, and contact e-mail beneficiaries will have to pass verification themselves – we will send them a notification and link.
- Also, we will need your CEO's (and other top managers) contact e-mail.
- Any company is a group of people (KYCs), including its ultimate beneficiaries, and of course those working and managing it.
- In terms of beneficial ownership compliance rules, most regulators require companies to disclose information about any shareholders with a 25% stake or higher. In our case for higher-risk clients, we'll go from 10% and higher.

What else could we ask about ownership structure?:

- Our system is designed as the following: during each encounter with a new "company as a shareholder" entity, it "loops" and "knocks inward" to disclose every shareholder with any number of shares – until only real people are left.
- The user who fills in the registration form doesn't have to provide all data himself – only contact e-mail of a shareholder for the system to contact and ask them provide more info on themselves.
- Each new participant needs to share information personally and nobody can do it for him or her – because it is very important that the person sitting in front of the screen is transparent in order to build trust.

What else can we ask?:

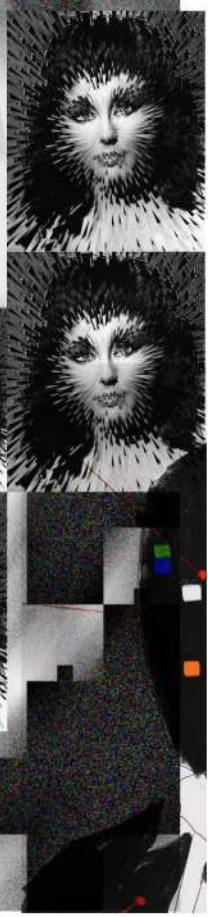
- Users can fill in all employees – and ask them to pass verification individually. One of the most common frauds includes 3-5 people making a gorgeous presentation where they put pictures of non-existent or fake 'employees'. In this case, we might want to make sure that apart from the owners, there are other employees within the company, competent and capable of bringing their plans to life.

  The same can apply to independent advisors and mentors – if you use their names in public material, we would like to know more about them.

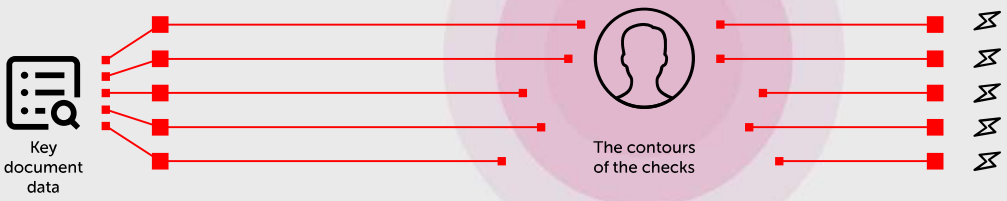
EDD

(Enhanced Due Diligence)

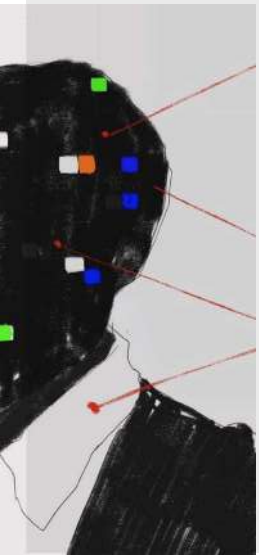
- If your business requires a special license in your country, we will ask you to provide it as well.
- What we already asked your end users as part of EDD:
  - + During KYC: bank card verification, social network accounts, relatives and biometric data;
  - + During KYB: every shareholder with more than 25% (or 10%) ownership, verification of all employees, mentors and advisors.
- For a better understanding of your business, we request additional materials, if you have any of them:
  - whitepaper,
  - business plan,
  - product or business presentation,
  - legal opinion,
  - team presentation,
  - investment deck.
  - we don't ask you to create anything new specially
  - for us – we simply ask you to share what you already have
- We might ask you additional questions on your source of funds and source of wealth. If you handle money from third-party individuals or businesses, it is crucial that it is verified.



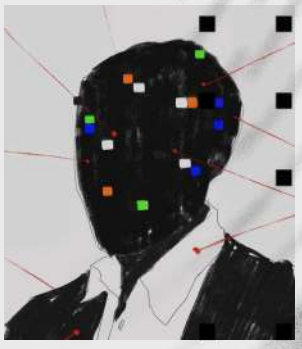
Ongoing Compliance



- According to statistics, real big fraudsters don't get caught during the stages of registration or onboarding – they learn to bend the rules. Transactions make it possible to track and catch them. That's why the ongoing compliance module is crucial.



- Based on the information we receive about the company during CDD and EDD, we will #hashtag many different parameters about you (and later compare with #hashtags of each new transaction):
  - your estimated expenses and items of expenditure in the future.
  - countries of consignment and destination
  - purpose and frequency of payment, etc.
  - In a situation where your company has suspiciously frequent and large transactions, the system will rely on these tags to decide whether this information complies with the information you stated during onboarding.



Ongoing Compliance

Thus, our clients have active accounts, and any other parties – <u>passive accounts:</u>

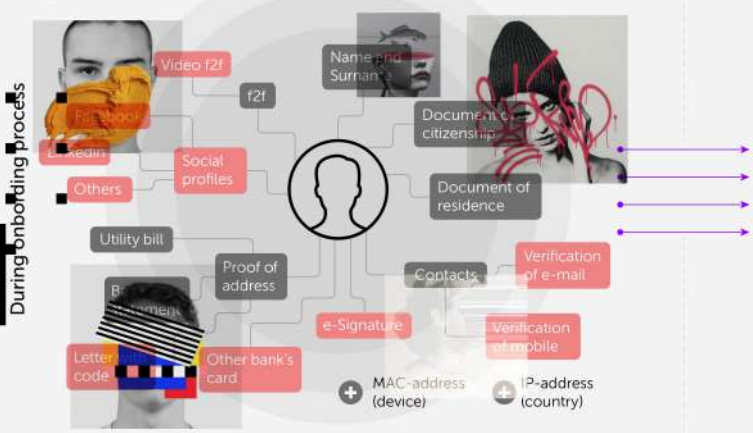
- We treat 'everybody' as 'users' including those direct and indirect (we create "passive" profiles accordingly) i.e. someone that encounters your bank during transactions:

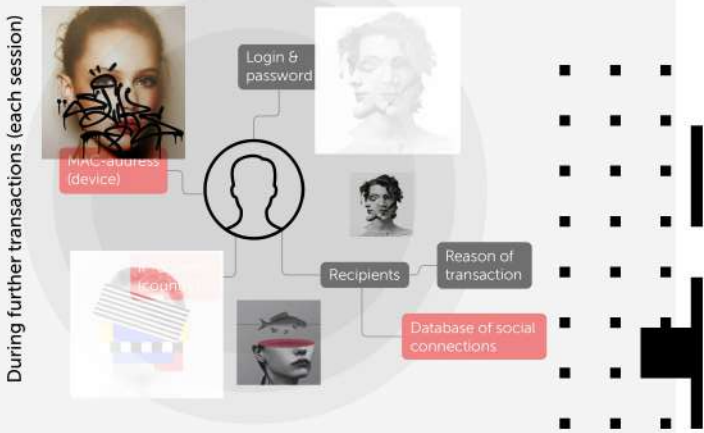
  01 - somebody sends money to your client,
  02 - receives transfers from your client,
  03 - a shareholder or a counterparty related to your client or
  04 - friends

- and colleagues from social networks - as soon as the system sees a new name or entity, it creates a new "container" and fills it with new data, one piece at a time.

> *When a new box is created, the system automatically tracks activities related to it. For example, our 10 separate clients have sent money to an external company – the trigger works, and the system automatically starts to search for additional (public) information about the counterparty. If information is unavailable or negative, it automatically sends the recipient a notification to pass an additional verification with us. The same works for money senders.*

Ongoing Compliance





Our system is built on **the principle of constant data triangulation:**

01 what we know about the company in general (original data base),

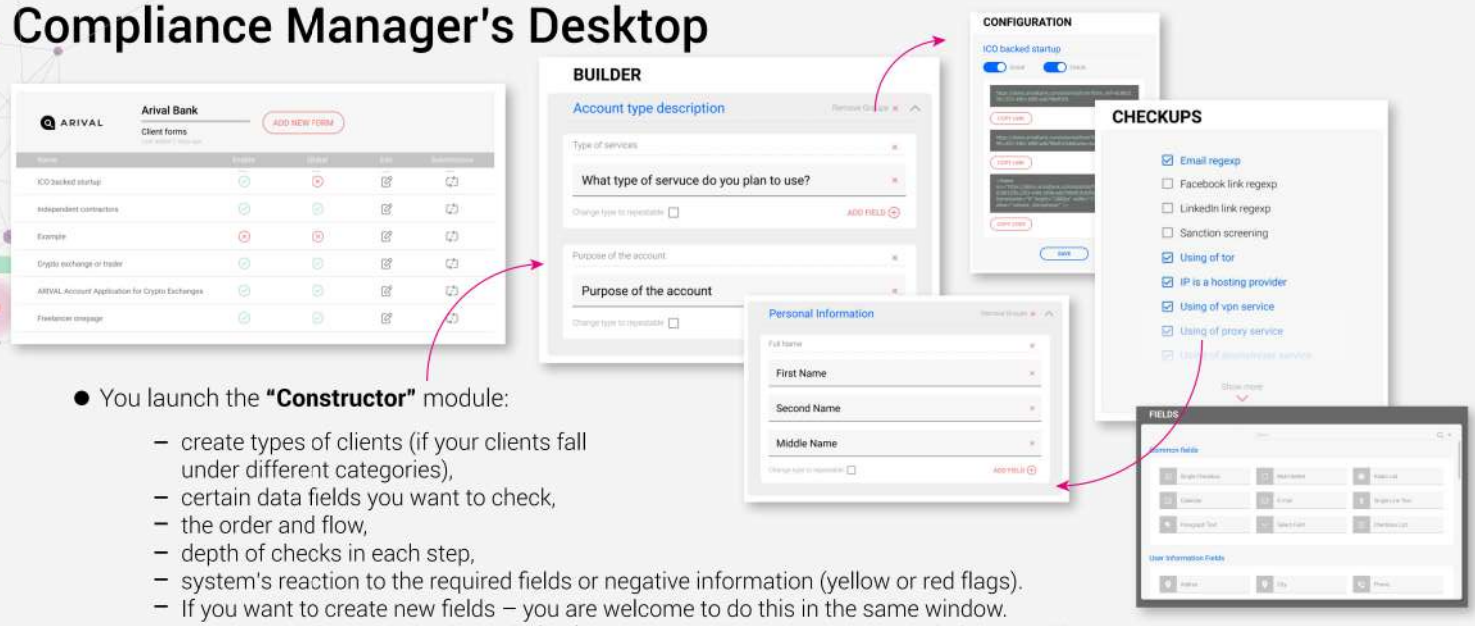
02 who operates in its name and what they do exactly (country, device, time, type and frequency of actions),

03 social and economic connections around the company and the person behind the screen (friends and colleagues from social media, money senders and recipients from other banks, shareholders, management and employees of the company).

BTW ↓

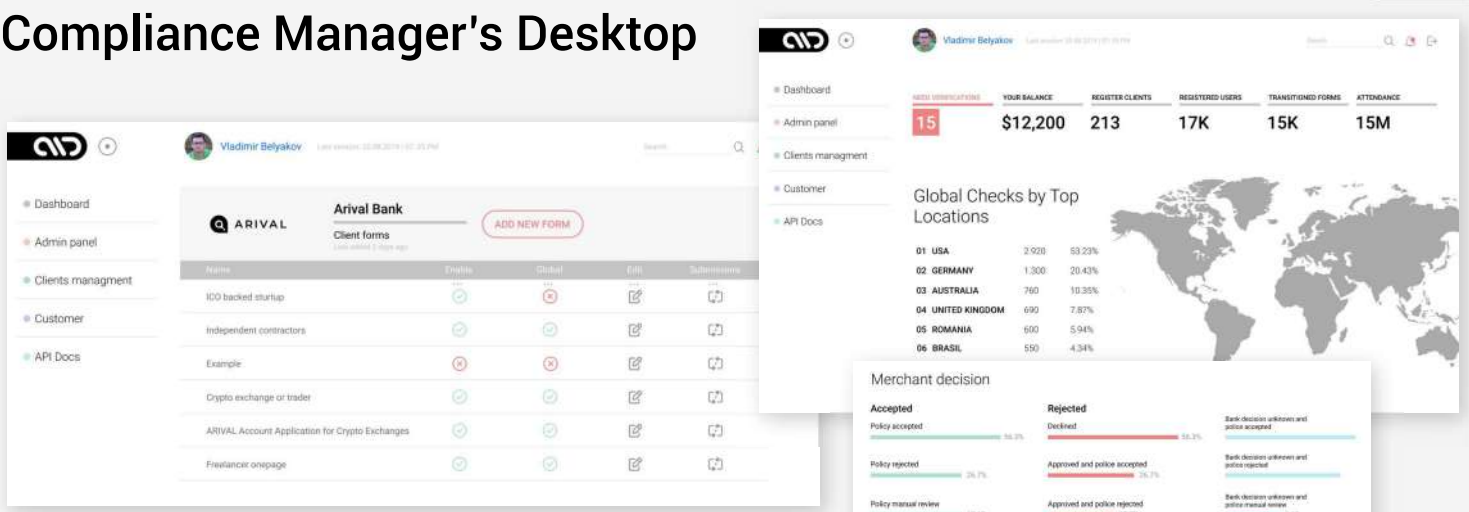
Professional fraudsters have long learned to bend banks' verification systems, providing suitable answers, clean shell companies and reasonable transaction goals – thus, it is much more efficient to track them implicitly, on the meta data level: general non-obvious social connections, similar behavioral patterns among non-related clients, etc.

Compliance Manager's Desktop



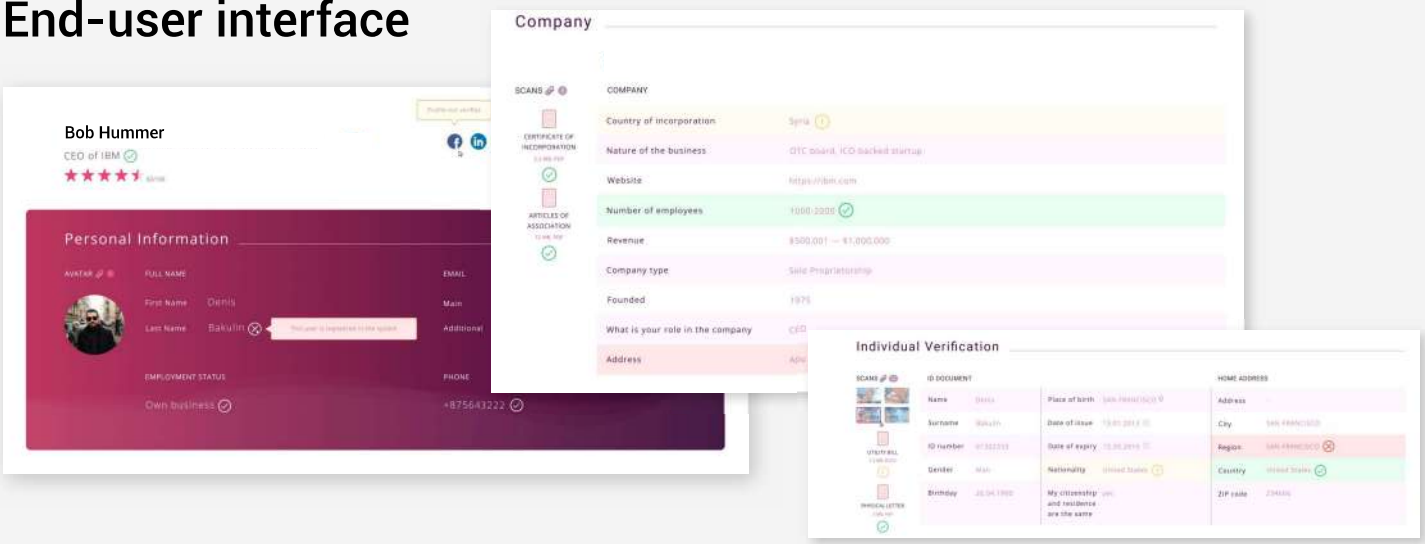
- You launch the **"Constructor"** module:
  - create types of clients (if your clients fall under different categories),
  - certain data fields you want to check,
  - the order and flow,
  - depth of checks in each step,
  - system's reaction to the required fields or negative information (yellow or red flags).
  - If you want to create new fields – you are welcome to do this in the same window.
  - Let's go! You have received a code (API) you now need to paste on your website or mobile app.
- Now the client sees a "Log in with A.ID" button on your website – if he has already passed the verification elsewhere, he simply logs in, if not, the registration procedure starts.

Compliance Manager's Desktop



- The actual compliance manager needs to pass the same verification process in the system as their future clients.
- As a compliance manager, you see the key metrics on the dashboard: how many clients have started the registration process, how many of them passed it, the clients you have approved and rejected. You can see the yellow and red flags and ask additional questions.

End-user interface



- We understand that we aggregate a lot of data – but to work with higher-risk clients, we need to trust them, and to be able to do this we need to see that the company and its representative are open to transparent dialogue.
- But we understand this amount of personal data is very sensitive.
- *That's why we create a separate interface for users – you can always see what information you provided to us and when, who else requested it (with your permission or refusal), what details, whether it is stored it or not – and make an automatic request to have it deleted.*

What is next?

- We have created our own internal **policies** - and we want to help you with:
  - Core System Task Analysis;
  - BSA/AML Risk Assessment;
  - OFAC Risk Assessment;
  - AML Risk Model;
  - Account Monitoring,
  - Investigations and SARs;
  - CDD/EDD/KYC module;
  - Vendor Management;
  - PDSA (Plan, Do, Study, Act) Cycle;
  - Cybersecurity;
  - Reputation Risk Management
- We want to **add more and more third-party verification services** to each step of our onboarding process and ongoing compliance and AML – there are many databases in the world, old and new, that check different parameters, and even new startups and technologies are emerging that take a single verification step to a totally new level;
- We want to make **the creation of risk-profiles** not constant, like they are now, but dynamic – to make it possible to create new scripts for different participants;
- **Interfaces for compliance managers require further elaboration** – not only to clearly see the triggers during onboarding, but also to be able to react to these flags instantly during transactions, ask clients additional questions and analyze the answers at once;
- When there is more data, we want to **integrate a neural network and artificial intelligence.**

> *At the moment our system works on our own questions and answers – the good analogy is "What is a cat? It is a small fluffy animal with four paws and a tail." But this approach excludes bald cats, or cats without a tail or a paw. Machine learning enable neural network to show one or two hundred cats at once, and the machine determines itself what a cat is. More than that, it constantly adapts its answer on the basis of the new data. And then, it learns to ask the questions itself, to group it automatically and to create new risk profiles.*

- We would like to help our clients not only technology-wise, but also with doing our own higher-quality **audit** of their compliance, as well as provide services for regular **training and skill development.**

Our long-term vision: identity is the new money

Inspired by the vision & thoughts of our friend **David Birch**, the author of the best-selling Identity Is **The New Money:**

David Birch

Author, advisor and commentator on digital financial services

- The social anthropologist and money historian Jack Weatherford wrote that ancient society worked on a shared memory of mutual cross-obligations, continuously adjusted and revised. Once clans form into tribes and tribes move into cities, the shared memory is no longer sufficient. We need intermediaries to manage, and money is one of them.
- The book "Debt: The First 5.000 Years" by anthropologist David Graeber argued that historians and economists have wrongly assumed that money grew out of barter. In fact, barter was never common and money was actually an evolution of credit-a way of tracking what people owed to each other. People used to just keep a mental tally of what they owed each other, but money provided a way to expand the system more broadly among people who didn't know each other. It served as a sort of physical ledger on which society could keep track of who was owed what.
- However, technology gives us back that shared memory, then we don't need intermediaries to enable transactions.
- It becomes what some people call a "reputation economy" (with credit-based nature of money) - this idea is very close to "human capital contracts" (or "social financial agreements") concept, which have been proposed by esteemed economists including Milton Friedman,
- This "social identity" is the basis for a reputation economy, an economy based on trust. It will be reputation rather than regulation that will animate trust in economic exchange, and that social graph, the network of our social identities, will be the nexus of commerce, administration and interaction. Thousands of 'currencies' based on your identity can bloom.

Correspondent banking bridges

Analysis and research by Vladislav Solodkiy
'October 2023

Building the first digital correspondent banking network for digital banks, EMIs, IFEs and e-wallets

"Fintech has disrupted many banking verticals, but (digital) correspondent banking remains an untapped niche."

Correspondent banking market highlights

There is a huge demand, lack of supply chain, significant problems from customers, a crazy payment volume, a high-margin business, and zero acquisition cost if you have anything to suggest.

There is no digital correspondent banking platform tailored to digibanks, EMIs, e-wallets, IFEs, & MT\MSBs

There is no correspondent monoliner that thinks about (bank-clients and) **end-users**

There is no direct two-way correspondent banking payment rails with integrated **compliance** orchestration engine

Problem

Corrbanking drawbacks slow down financial flows

Banks, digital banks, & neo-banks are rapidly evolving & entering the market.
The Correspondent banks they use are not. The supply for fintech stays the same.

The current system lags behind its potential due to:

Time-consuming relationship setup[5]
- Offline onboarding[6]
- Calls, meetings & document ping-pong
- 6-9 months to fully operational CBR[7]

Developers-unfriendly old tech[8]
- No APIs
- No SDKs
- Offline support[9]

Secured deposits model hinders speed
- No trust
- No transparency
- No efficiency or flexibility

Compliance nightmare
- Large trx freezes
- Manual processing[8]
- Trx pending status up to 12 weeks

Correspondent banking challenges | Real customers' pain

The problems after SVB, Silvergate, and Signature banks have made demand even higher

No need to replace your core-banking and compliance systems - we are integrating (mirroring and sync) on top

APIs & Clear integration documentation

Fully-digital onboarding process

Clear proposal and expectations

Transparent requirements

Online documents submission & application approval

Plug'n'play ready-to-go tech.integration

Direct buffer accounts monitoring

Orchestrating core-banking systems

One compliance language (translation) for all chain participants

✓ **KYCC problem solving**

Dedicated dashboards for each corrbank. Direct CB-to-client messaging. Full browsable trx history

Orchestrating compliance systems

Opportunity: It is a real cash cow and can quickly become operationally profitable, which is critical in the current economic situation.

A lot of money to be made yet noone is interested

79% of value in CB trxs is moved by correspondent banks, generating **$150+B revenue** p.a.

4 out of 5 FIs process international trx through corrbanking channels[3]

But for no bank CBRs are at the core of their business model. They are retreating and scaling down (see our research).

CBRs are hard to establish and very expensive to maintain

SWIFT provides the information but doesn't provide the payment rails. (see the model). Each new legacy CBR requires tailored complex tech integration.

SWIFT works only one-way and relies on the pre-loaded deposit model which needs constant monitoring and forecasting, creating **liquidity collapses**.

Costly compliance slows down the most fast-growing segments (ecom, fintech, crypto, trade finance) (see research). New **AMLA regulations of Jan 2024** make it even worse. ✓

starting from January 1st, 2024, FinCEN is introducing a new regulation, AMLA, which requires banks to conduct KYCC, which affects correspondent banks the most

Competition

New entrants only offer band-aids and target different markets

	Legacy corrbanks	Fintech	Blockchain solutions
Motivation	CBR as **a tertiary revenue stream** leveraging their convenient geo location	Focus on the **end-user pains**: to speed up small transactions for smaller costs	DLT creates streamlined trustless flows in **disparate siloed networks**
Drawbacks	Offering CBR within current system with their tech and risk-based assessments are not profitable.	Lack of licence leads to compliance challenges, limits clientele and trx processing capacity	Build tech with no focus on banks-clients, ignoring legal aspects and other industry pains and specifics
Target market	**Low-risk banks & FIs**	C2C, B2B, P2P	Banks, FIs, B2B, P2P

There are around 550+ competitors across the globe, including the two largest (JP Morgan and Deutsche Bank) and the five banks we are connected with, however, none of them are fully focused on this business.

digital banks, European EMIs, Asian e-wallet giants, Puerto-Rican IFEs, MTs\MSBs, and brokers, all facing the same and the same issue

Ripple have chosen XRP games over correspondent banking, and do not pay close attention to compliance. Ripple works for small crypto-related transactions but is not a wholesale solution.

Fintech has disrupted many banking verticals, but correspondent banking remains an untapped niche.

Like “Wise for banks”: on the way to digital correspondent banking

Built-in compliance

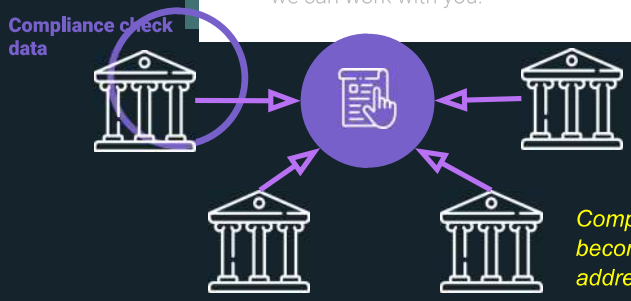
No more Chinese Whispers — universal compliance workflow allows YOU to onboard:

- **FIs from high-risk jurisdictions**
- **Banks that serve high-risk clients**
- **Digital banks with unconventional business models**
  No matter how innovative you are we can work with you!

Seamless and quick FIs onboarding

API-integration allows to establish CBR with ease:

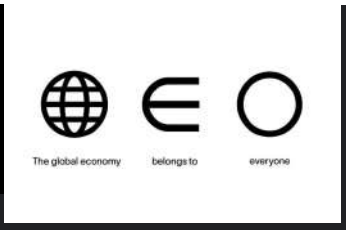
- **All integration terms are available online**
  No more phone-call Odyssey and dismissed requests
- **Transparent onboarding process & requirements**
  No more unexpected surprises or hidden costs
- **Online document uploading & quick decision-making**
  Integration will take weeks instead of months



Compliance requirements from regulators have become more stringent, making it impossible to address this as an ad hoc business.

Correspondent banking as a client acquisition channel for the digital identity product

Like Worldcoin, but useful



Your correspondent bank-clients store tons of data about their end-users (senders and recipients), including images of IDs, real-time photos and videos, social and business connections, presentations and docs, reasons for transactions, etc.

You generate thousands of new government-accepted KYC-ed profiles for end-users, which could be an amazing basis for services like digital identity (online-voting and elections, automation of visa-application processes, check-ins in airports, and more).

Complimentary products

- Sweep Deposits program
- BaaS for fintechs
- Smart Treasury (beyond Fed rates)
- Paid-in capital loans
- first CBDC-friendly bank
- Digital Identity solution for end-users ✓
- Cross-border Stablecoin Issuance
- AI-fueled AML engine

Must have: you also integrate compliance to avoid stuck transactions, which is a significant problem for all correspondent banking providers

Players do not serve high-risk clients due to compliance nightmare

>$270B
compliance costs
per annum[16]

up to **$4B** p.a.
for one bank[17]

Compliance costs each bank **4-10% of revenue.**[16]

60% of CB B2B trx are processed manually for at least 20 min.[8]
It makes **1.5M+ FTE per year globally.**

~5% of all cross-border trxs cost banks 25x–35x more in compliance than in processing[17]

Correspondent banking is not just about payment rails, but it also involves the orchestration of core-banking systems, compliance systems, and knowledge of the regulatory requirements in the US (as the main corridor for correspondent banking services).

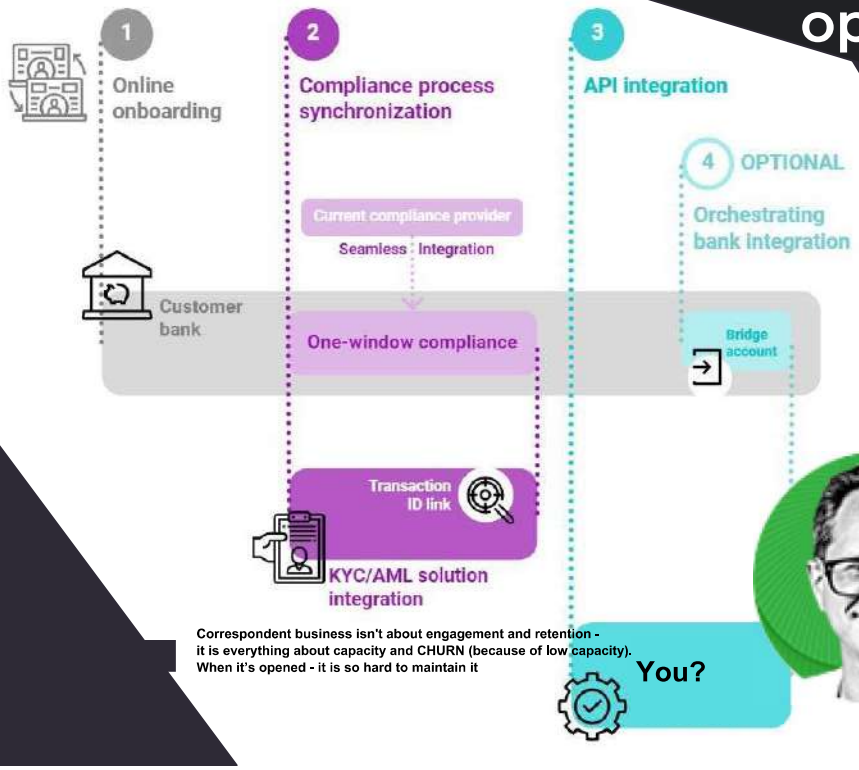
Chinese Whispers problem

Jurisdictional legal restrictions[1], varying compliance processes and requirements, and manual data handling lead to the loss of compliance data and slow processing

1 — Many respondent banks **may not lawfully share** certain types of customer due diligence data with corrbanks due to strict data protection and bank secrecy laws.[6]

Pain: NO ONE 100% happy with their current correspondent bank provider - this is why everyone is always looking for 2nd, 3rd, 4th partners (just in case and to avoid dependency)

Target: Correspondent account opened within a month



1. You fill **an online form**, directly uploading all digital documents into our system
2. You install **our compliance solution** that integrates your current provider into the database and the user-friendly interface.
3. **You** connect clients with your Platform **via our high-throughput API**.
4. **To eliminate secured deposits** you install our core on top of your infrastructure
already work with many: C
Evolve, Mbanq, Railsbank, Contis

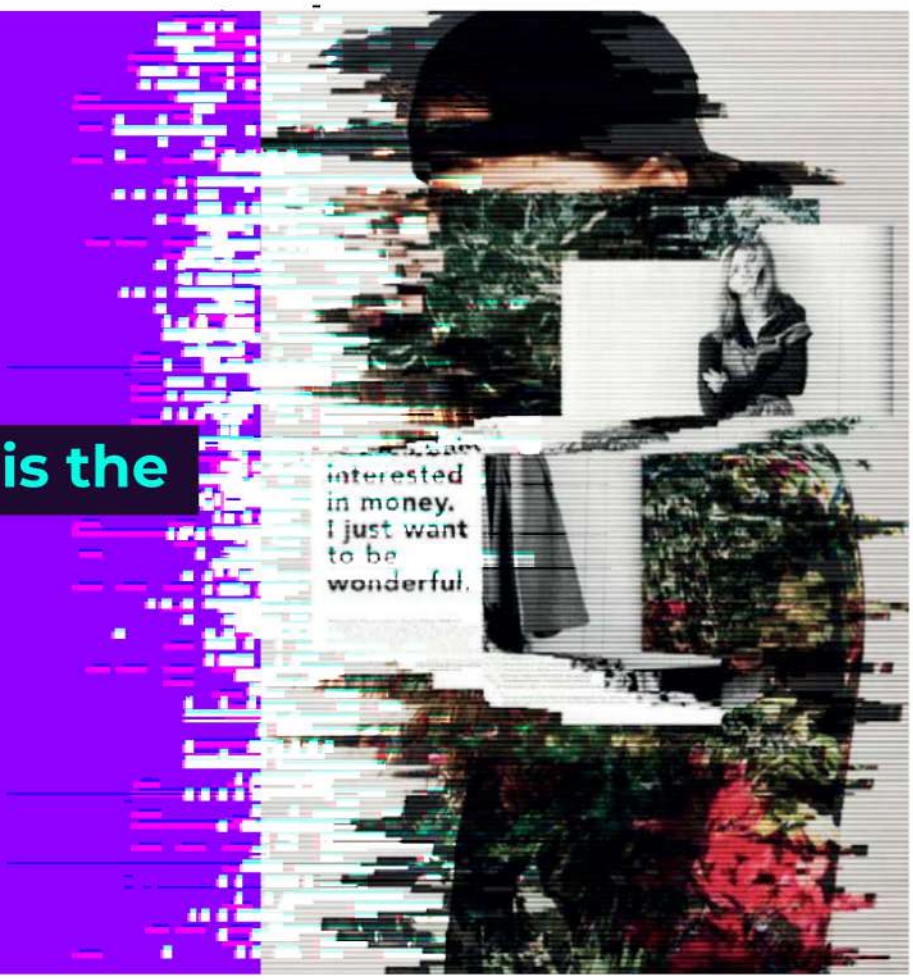
Correspondent business isn't about engagement and retention - it is everything about capacity and CHURN (because of low capacity). When it's opened - it is so hard to maintain it

Correspondent banking isn't a favor, but a service

POWERTO
R ICO

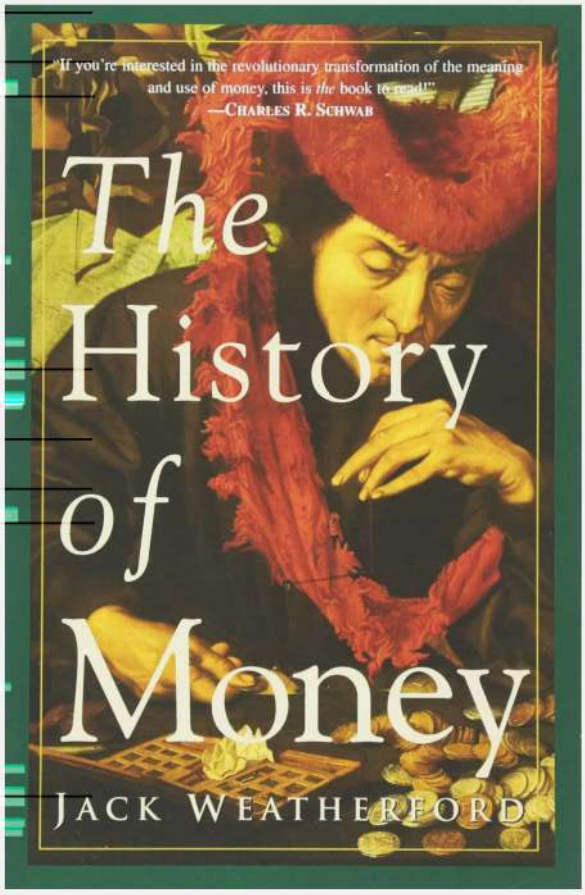
Blockchain {$powered;
territory'//>

[Digital] Identity is the new money



THE
FIRST
FINTECH
BANK

ARIVAL

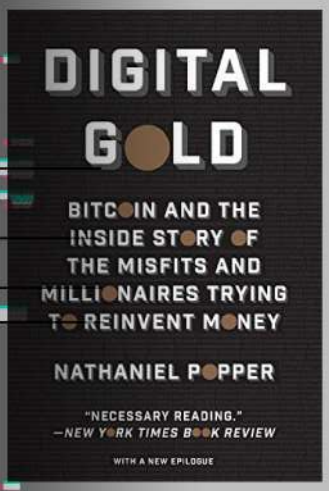


The social anthropologist and money historian Jack Weatherford said: "The electronic money world looks much more like the neolithic world economy before the invention of money than it looks like the market as we have known it in the past few hundred years."

What Weatherford means is that ancient society worked on a **shared memory of mutual cross-obligations,** continuously adjusted and revised.

In the clan, everyone knew who owed what and to whom, a structure that does not scale beyond the kinship group. Once clans form into tribes and tribes move into cities, the shared memory is no longer sufficient.

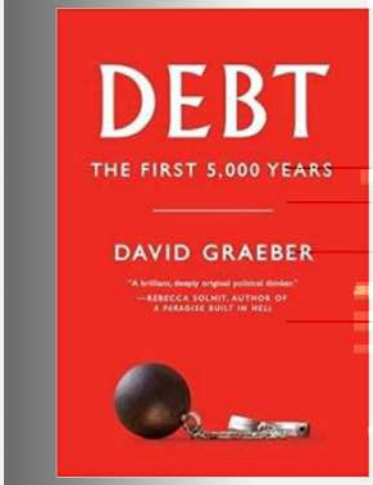
We need intermediaries to manage, and money is one of them. If, however, technology gives us back that shared memory, then we don't need intermediaries to enable transactions. It becomes what some people call a "reputation economy".



Nathaniel Popper mentioned, "the book by anthropologist David Graeber, argueds that historians and economists have **wrongly assumed that money grew out of barter.**

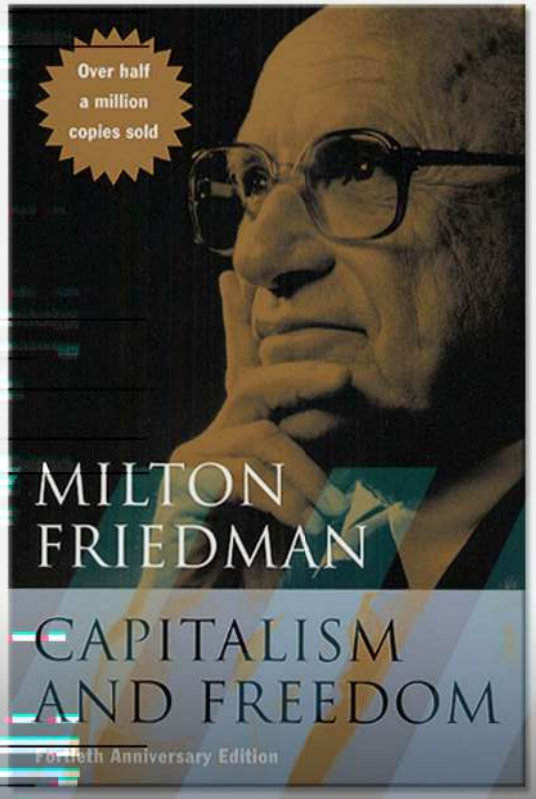
In fact, Graeber argued barter was never common and **money was actually an evolution of credit - a way of tracking what people owed to each other.** People used to just keep a mental tally of what they owed each other, but money provided a way to expand the system more broadly among people who didn't know each other.

The reason gold itself had been used as money was not that it was valuable, **it had become valuable because it was used as money**. And it was used as money because it did what all good money did: it served as a sort of physical ledger on which society could keep track of who was owed what. Each piece of gold represented a slot on the ledger of all outstanding gold, which anyone could verify by checking the mass and volume of the gold.



Money in its current manifestation is broken.

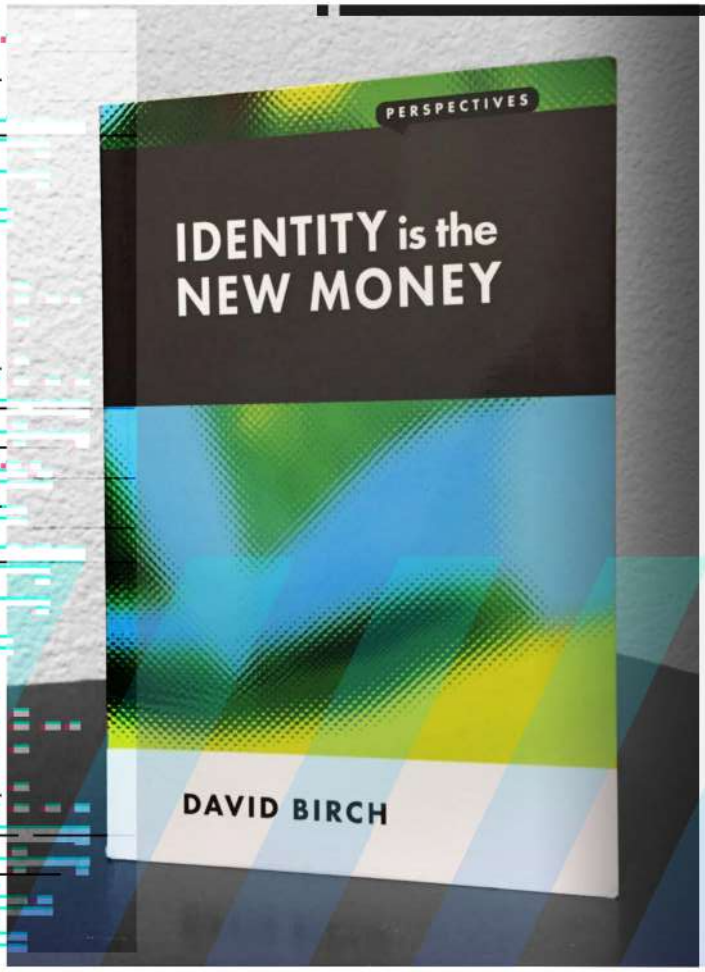
Barter was never common and money was actually an evolution of credit-a way of tracking what people owed to each other. As David Birch wrote: "The social anthropologist and money historian Jack Weatherford said: "The electronic money world looks much more like the neolithic world economy before the invention of money than it looks like the market as we have known it in the past few hundred years." What Weatherford means is that ancient society worked on a shared memory of mutual cross-obligations, continuously adjusted and revised. **Technology gives us back that shared memory,** then we don't need intermediaries to enable transactions. It becomes what some people call a **"reputation economy", which is based on "social capital"** (the result of computations across the social graph).



"The human capital contracts" (or "social financial agreements") concept, which have been proposed by esteemed economists including Milton Friedman, who advocated them as an alternative to taking on student loans.

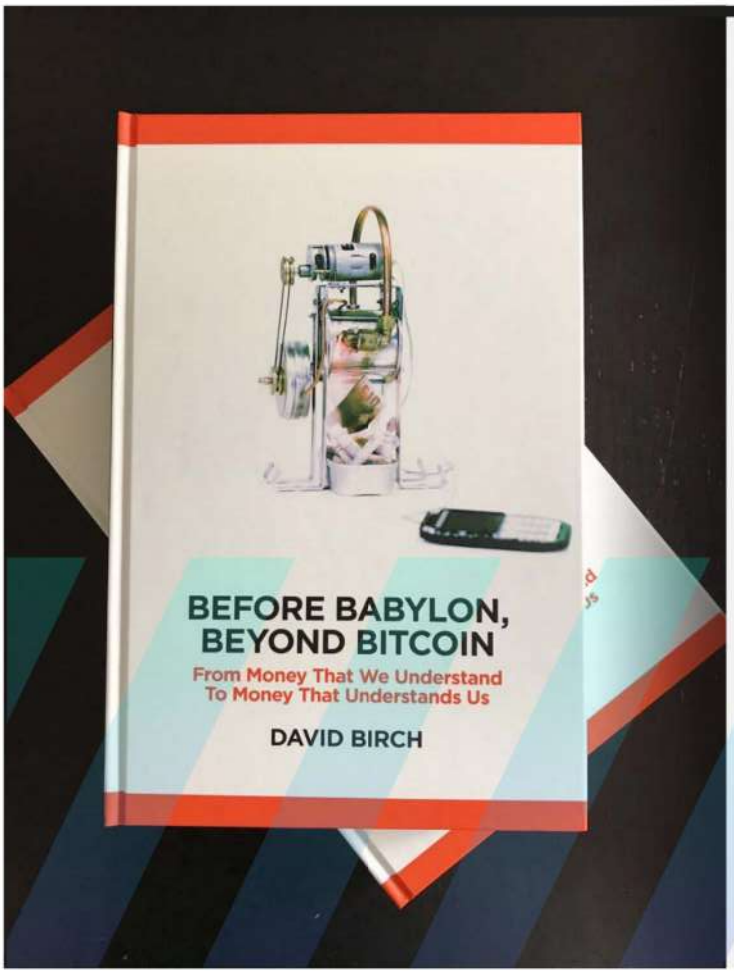
Yale University even experimented with them before the federal government started guaranteeing loans. The concept has been compared to artistic patronage, as when wealthy merchants funded artists in Renaissance Italy in exchange for prestige, artistic influence, and a collection of works that could climb in value.

Today, it's common for tournament poker players to raise money from backers in exchange for a cut of the winnings.



The idea of "reputation economy" by David Birch (with credit-based nature of money and human relationship by David Graeber) is very close to "human capital contracts" by Milton Friedman. Birch is continuing this idea: "Using patches such as college degrees and credit ratings instead of real, immediate reputational data is just not good enough in our connected world, which is why there are companies now looking at using the social graph as an alternative."

"Social capital (the result of computations across the social graph) is now accessible and usable at the transactional level. Proxies such as high-school diplomas and glossy CVs are being replaced by social capital **because it is a more efficient form of the kind of memory** we need to make transactions work."



"With that kind of transactional **social capital in place, delivered by the combination of mobile phones and social networks, commerce will be reinvented.** That social capital will be deployed in smaller and more commonplace transactions, not only getting a job or buying a house. In the long run there will be no need for a single medium of exchange, no need for fiat currency."

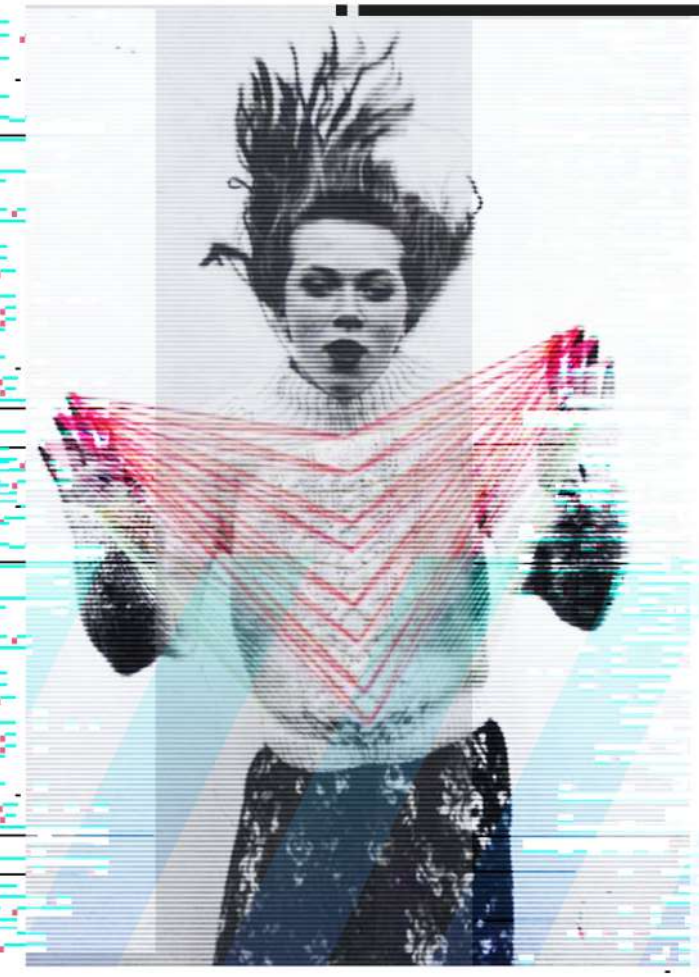
"This **"social identity" is the basis for a reputation economy, an economy based on trust.**

It will be reputation rather than regulation that will animate trust in economic exchange, and that social graph, the network of our social identities, will be the nexus of commerce, administration and interaction." In such a world, **cash is no longer needed, and thousands of 'currencies' based on your identity can bloom.**

""Social identity" is the basis for a reputation economy, an economy based on trust. It will be reputation rather than regulation that will animate trust in economic exchange." Regarding idea of David Birch, that in such a world, cash is no longer needed, and thousands of 'currencies' (your own currency or Google\Facebook\Apple-currencies) can bloom. **"We can only hope that the giants like Apple and Google will one day be fully independent from the governments that hinder the embodiment of their ideas. It is possible to achieve this work, if they will create their own independent state,"** — ponders the creator of VK and Telegram Pavel Durov.

Building the puzzle of the ecosystem: big data as a «blood system»

- Observing actions of big centralized credit bureaus obviously realize that the market is changing (especially in Asia), as traditional approaches do not allow these giants to tackle their new clients' problems in an efficient way. **Traditional credit scores are but one indicator of overall well-being.** But there are other measurements that also matter to both consumers and providers. How are people doing managing their daily finances? Do people use systems and products that make them resilient to unexpected financial c hallenges? Are people able to achieve major financial objectives — such as buying a house or retiring comfortably?
- **Data is the new money.** Big data is a connector between all fintech verticals and other industries. We can (and have to) analyze **unstructured data from various sources** – bills payment, mobile calling patterns and locations, insurance premium payments, social media profiles and check-ins, thousands of data points, everything from a smartphone user's messaging and browsing activity, to the apps and Wi-Fi network we use, – to provide meaningful social scores for retail customers and SMEs.
- **People are more than just their credit scores. Identity is the new money** – like «human capital contracts» (or «social financial agreements») – for reputation economy. «It will be reputation rather than regulation that will animate trust in economic exchange, and that social graph, the network of our social identities, will be the nexus of commerce, administration and interaction».



Data is the new money, and data — like money before it — is only valuable if it's being shared and rehypothecated through the wider network. Furthermore, we put our data into the safekeeping of cloud custodians for precisely the same reasons we put our money into the charge of banks: security, liquidity and utility maximization. Are Deloitte, Yahoo, and Equifax too big to trust? Do they really care if your data is exposed?

Maybe we should put all data on a blockchain, decentralizing the system and querying discrete pieces of information as needed. But all this breach should wake us up to how fundamentally broken this system is, and how urgently we need to replace it. Breaches aren't simply security failures; they're the inevitable result of a broken data storing system by traditional big institutions.

New challenge: how to keep personal information safe?
Even big players and governments cannot deal with the problem.

Credit losses due to identity theft exceed $20 billion each year and these are considered losses for regular people, not banks. Mostly due to human factors, like sending sensitive data in non-encrypted e-mails, merging and matching data from different verification providers manually, etc.

US, 2017

- 143 million US customers
- Equifax
- Birth dates, credit card numbers and more

Sweden, 2017

- 6 million Swedish citizens
- Swedish government
- Names, photos, home addresses, details on every vehicle in the country

Singapore, 2017

- 5400 Singaporeans
- AXA
- Email addresses, mobile phone numbers, insurance policy numbers and dates of birth

What about digital identities on blockchain?

There are a number of industries that "print money" by selling to a captured market - one of these industries is the credit reporting industry. **Do we really need Equifax (the company announced that the total number of people impacted by its breach is not 143 million— but in fact 145.5 million), Experian, Transunion, etc, if they are not protecting our data and identities?** Your data should be free for you and expensive for others. Putting consumers back in control of their financial data on the way to "social capital" system. Seems the biggest issue for cryptocurrencies and ICOs is KYC\AML\"source of funds" questions. Such approach like blockchain-based digital KYC\AML (or even **"reputation economy" based on digital "identities" with connected "social capital"**) can help to solve this issue.

As most of the world population remains unbanked, the challenges of lending and scoring are more critical than ever before. Traditional scoring does not work- even in the US

Monopoly of few organizations:

Still on many markets credit scoring is a monopoly controlled by one or few organizations. Traditional credit bureaus require borrowers to take on debt before obtaining a credit score, leaving millions of potentially creditworthy individuals unscorable by the current credit system.

Invisible Americans:

People stay credit invisible even in the US. The number of credit invisible Americans exceeds 25 million. To become banked they are forced to borrow at highest possible rate – which makes them even poorer than before.

Poor people without bank accounts stay poor:

Globally, it is much worse. 38% of the world's population does not have a bank account. 3 billion people are unable to obtain a credit card and 91% of residents in developing nations experience difficulty receiving debt financing from traditional financial institutions.

Siloed markets:

Credit scoring is siloed around the world, further exacerbating these issues. Credit scoring providers can not operate globally, meaning that for a new market they must rebuild their credit scores from scratch. There should be one uniform regulation created to cover all the world.

Identity is the new money. Single digital ID\KYC – it's not a dream about the future, it's already a reality, with which you still can not reconcile and finally do it. **Blockchain-based fully digital Identity is the essential standard of today.** The verification should not have geographical boundaries. Digital KYC should be available not only for people, but for businesses as well. Look at projects such as E-Residency in Estonia or Atlas by Stripe - why is it working for them, but not for us? We want to establish a "company in the cloud," or opening an "account in the cloud," and provide services to people in different countries and allow them to move freely. **Not only verification, but scoring, should also get rid of geographical boundaries.**

Blockchain Future: Customers control who they share digital identities with...

Customers directly control to whom they share their personal information and documents, keeping track of these authorizations in the distributed ledger using smart contracts

Secure

Removes the need to trust third parties. All logs are stored in the ledger distributed between multiple authorised parties.

Auditable

Uses the blockchain technology to ensure that once written, information is not altered or deleted, even by system administrators.

Fair

Uses billing based on the blockchain records. There is no need for additional verification. Counterparties have access to identical records.

The legacy financial system is like holy condoms put on one another. **We need open architecture only.** Monopoly over infrastructure is evil. Modern services should be able to communicate through the open API. In the world where almost everything can be found on the SaaS model we need bank-as- a-service platforms, broker-as- a-service, insurance-as- a-service... By the way, **what about government-as-a-service?** For example, from Estonia or Singapore. Judging by the reaction of some countries' regulators to innovation - the world will only benefit from this.

Solution

Unified digital ID

- Passports, visas and other documents. Unified digital IDs (like the ones they have in India): no need to fill in forms multiple times and wait for weeks before the documents are ready. And, of course, no need to bribe officials to accelerate the process or get fake documents.
- Significant decrease in "parasites": useless middlemen like officials, passport office and Pension Fund workers...

Unified digital ID

- Registration and confirmation of personal data. Blockchain-based identification management. The solution to citizens' personal data theft issue.
- Integration with fingerprint scanners, voice and iris recognition and other personal biometric devices.
- Algorithms of user recognition according to personal gadgets connected with the system. This enables to achieve maximum level of integrity and operational compatibility within any infrastructure.
- There is a number of projects worldwide that cover the field of verification of authenticity and reaffirmation of access rights: 2WAY.IO, ShoCard, Guardtime, BlockVerify, HYPR, Onename, BAASIS ID, Civic.

Worldwide experience

- In 2016, UAE hereditary prince has approved state strategy for total conversion of state document management to blockchain protocol by 2020.
- Austrian company Neocapita has announced establishment of decentralized platform based on private fully-permissioned blockchain Stoneblock, aimed at solving the costliest problem of electronic government – creation of registries. Neocapita is negotiating implementation of Stoneblock platform in Afghanistan and Papua New Guinea.
- Swiss startup Procivis in collaboration with electronic government experts from Estonia has announced the launch of blockchain-based "app store" for electronic government by the end of 2017.

A BORDERLESS COUNTRY

E-Estonia is the most ambitious project in technological statecraft today, for it includes all members of the government, and alters citizens' daily lives. The normal services that government is involved with — legislation, voting, education, justice, health care, banking, taxes, policing, and so on — have been digitally linked across one platform, wiring up the nation.

Digitizing processes reportedly saves the state two per cent of its G.D.P. a year in salaries and expenses.

It helps to clarify the differences between a nation, a state and a geographical country. These things are already a bit fuzzy, but in general, a nation is a group of people within an area who perceive themselves as being the same type of person; a country is that geographical area itself; and a state is the set of political organisations that those people agree to adhere to. By disconnecting the silicon-based functions of the state from the actual soil-based country, Estonians are protecting their nation from fates that might befall their country.

Estonia is one of the first countries to start implementing blockchain on state level

- Estonia's statewide project of the unified electronic system is one of the most successful implemented projects in the world.
- The decentralized open system connects different services and databases. Because of this structure, it is easy to implement new services and applications, and their transition to blockchain system is fast and easy.
- "Cloud business" project in form of a e-Residence project was fulfilled.
- In 2017, as the result of 1.5 year-long project with the Estonian government and the Nasdaq stock exchange on a blockchain-based system for company shareholder voting, it was announced that the experiment was successful and its scope of application would be expanded.
- In the first half of 2016, the Estonian government agreed with Guardtime to transfer data of more than 1 million state citizens' medical cards to a blockchain database.
- 94% of citizens have electronic IDs that enable them to use the system. 2% of countries GDP is saved on a no-paperwork governmental system; 4000+ services are provided digitally; Estonia is the №1 country in the world by tax collection and Digital Economy Index.

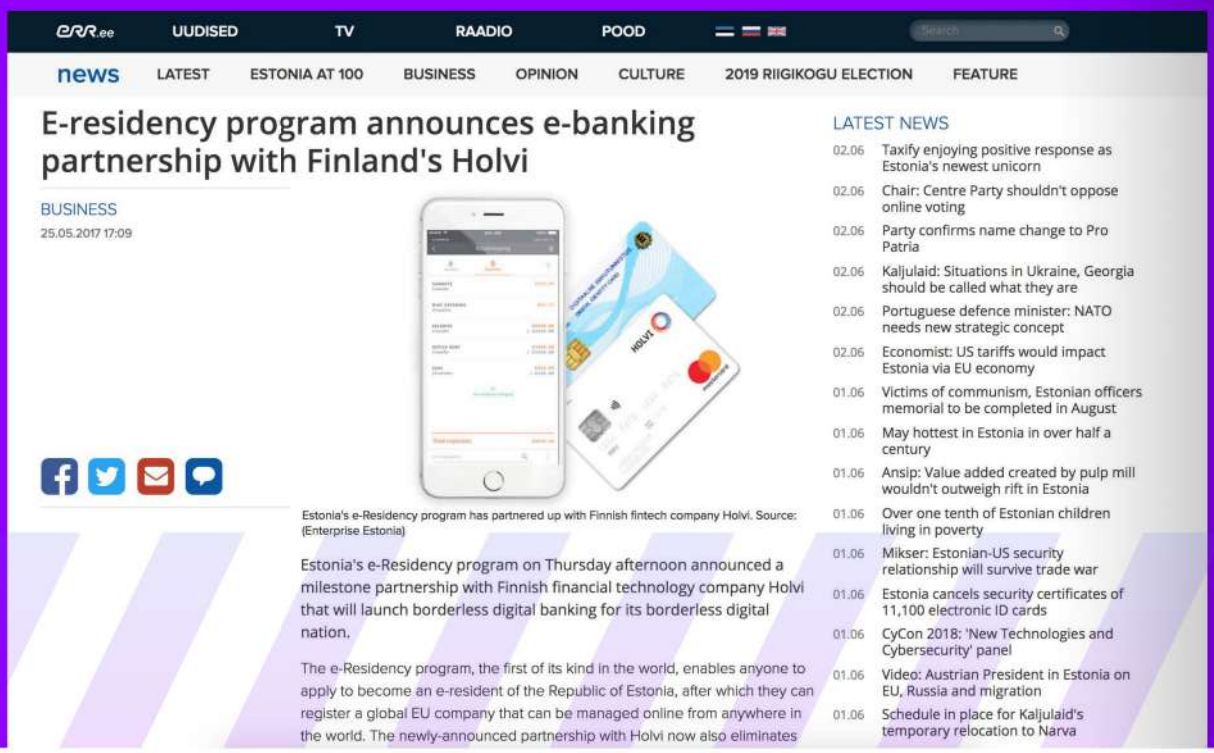
COUNTRY-AS-A-SERVICE

In 2014, the government launched **a digital "residency" program,** which allows logged-in foreigners to partake of some Estonian services, such as banking, as if they were living in the country. It permits citizens of another country to become residents of Estonia without ever visiting the place. The program allows individuals to tap into Estonia's digital services from afar.

Other measures encourage **international startups to put down virtual roots;** Estonia has the lowest business-tax rates in the European Union.

*"It makes it so that, if one country is not performing as well as another country, people are going to the one that is performing better — **competitive governance** is what I'm calling it," Tim Draper says. "We're about to go into a very interesting time where a lot of governments can become virtual."*

BORDERLESS APPROACH IS STILL VERY NEW FOR BANKS (AND REGULATORS)



«Simple banks» for SMEs and GIGs

	LIVE	HQ	Other markets	Clients	Banking license	Foreigners-friendly	Crypto-friendly	Integrations with 3rd-party fintechs	BaaS-platform for other fintechs	Funding
Holvi 2011	+		Europe	n\a	+	+ (via e-Residency program, excluding US users)	-	+ (mPOS: SumUp, few)	-	$4M total. Acquired by BBVA in 2016
Seed 2014	+		-	n\a	- (The Bancorp, "three deals with other banks")	+ -	-	-	-	n\a
CivilisedBank 2014	- soon		-	n\a	+	-	-	-	-	n\a
Tide 2015	+		- plans	30K+	- (e-money) (Prepay Solutions)	-	-	+ (lending: iwoca)	-	$14M (A) $16M total
Qonto 2016	+		-	5K+	- (Treezor)	-	-	+ (mPOS: iZettle, transfers: Kantox)	-	$11,3M (A) $14,3M total
Azlo 2017	+		-	n\a	- (BBVA)	-	-	+ (mPOS: Square, acquiring: Stripe)	-	n\a (backed by BBVA)
Penta 2017	Beta		- (Europe in 2018)	n\a	- (SolarisBank)	-	-	- (plans)	-	$2,7M (seed)
Arival Bank 2018	- soon		- (plans: Europe, Asia)	(waiting list)	- (applying)	+ (tailored for international businesses)	+	+	+	$1M on pre-seed ($10M raising now as seed)

Solution

Services for entrepreneurs

Establishments of legal entities, tax reporting, connections between companies and employees (vacations, employment records), contracts (agreements, invoices) among companies (and their enforcement) – everything can be tokenized for automatic record of enforcement, transparent enhancement and elimination of bureaucracy and corruption.

Worldwide experience

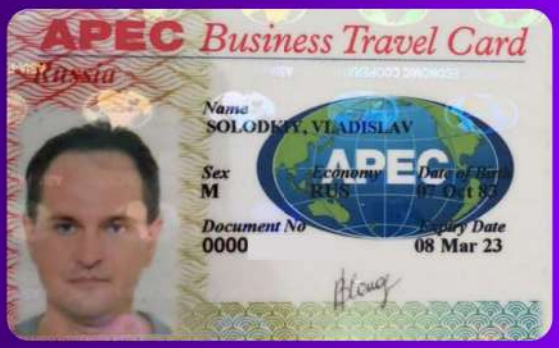
- Today there is already a number of successful projects for "cloud business" establishment (and they receive a bank account for it along with other financial services:

  - E-Residence in Estonia (bank account from Holvi 2 or Paywall 3)

  - "Atlas" product from Stripe 4 (registration of company in USA from any other country + account from SVB + acquiring from Stripe)

- In 2017, the state of Delaware (USA), presented the initiative to automatize juridical and operational activities of companies in partnership with Symbiont (a startup) and Pillsbury Winthrop Shaw Pittman LLP. The system digitizes the process of company registrations, tracking stocks movement and communication management of stockholders.

- Registration of companies and document circulation for business: for this purpose, there are such blockchain-services as Otonomos, BoardRoom and Colony.



The APEC Business Travel Card

...is a travel document issued to business travellers who are citizens of APEC participating economies. Valid for five years, the card eliminates the need for its holder to possess a visa when visiting other APEC participating economies as long as pre-clearance has been obtained during the application process.

Australia, Brunei Darussalam, Chile, China, Hong Kong, China, Indonesia, Japan, South Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, Vietnam.

After submitting an application, an applicant's name is circulated amongst the other participating economies which give entry pre-clearance when all conditions are met.

Solution

Unified social scoring

- Connection of all personal documents with credit history bureaus, mobile connection operators, social networks etc.
- Tracking behavior in online and offline services, encouragement of positive social behavior.

Chinese national scoring system

- To be Chinese today is to live in a society of distrust. It is China's ambitious plans to develop a far-reaching social credit system, a plan that the Communist Party hopes will build a culture of «sincerity» and a «harmonious socialist society» where «keeping trust is glorious».
- The ambition is to collect every scrap of information available online about China's companies and citizens in a single place – and then assign each of them a score based on their political, commercial, social and legal «credit». The idea is that good behavior will be rewarded and bad behavior punished.
- Under government-approved pilot projects, eight private companies (including Alibaba\AliPay and Tencent\ Baidu) have set up credit databases that compile a wide range of online, financial and legal information.

That project, launched in Jiangsu province's Suining County in 2010, gave citizens points for good behavior up to a maximum of 1,000. On this basis, citizens were classified into four levels: those given an "A" grade qualified for government support when starting a business and preferential treatment when applying to join the party, government or army; or applying for a promotion. People with "D" grades were excluded from official support or employment. The Suining government later told state media that it had revised the project, still recording social credit scores but abandoning the A-to-D classifications

China, «system of social trust» → (社会信用体系)

- Xi Jinping has begun his leadership in China with a tough fight against corruption in the Party, and now he aims at changing the society. With help of digital technologies and big data, the system analyzes data about each citizen, giving him individual scores. Technology giants like Alibaba\AliPay, Tencent and Baidu has helped him bring this project to life.
- Project has started in 2014 with adaption of "Program of development of Social Credit System (2014-2020)": by 2020, not only every company, but every citizen of mainland China will be tracked and evaluated by this system in real time.
- Trust rating is connected to internal passport. Ratings will be published in a centralized internet database with free access. Citizens with high rating will enjoy various social and economic benefits: cheaper loans, health care and education. Private companies provide discounts.
- Citizens with low rating are not accepted to various jobs, aren't given loans, can't purchase high-speed train and plane tickets, can't hire a car and a bicycle without bail, are restricted to leave the country.
- Companies are checked for their activities to follow ecological and juridical norms. Work conditions, workplace safety and financial reporting is being inspected. If there are no issues, the company is assigned high rating and enjoys privileged tax regime, good loan conditions. It can be placed on exchange and gets simplified administrative procedures, an "incomplete set of documents adoption" principle.
- Every official's personal data analysis: system compares data about the official and his family members' incomes with their data of real estate and luxury items purchases. This approach enables to predict official's behavior and reveal potential corrupters in a much more efficient way.

Big data and digital identities go beyond fintech... they can apply to just about every industry. Healthcare is an example of the biggest potential market.

Opportunities in health data:

- A complete data storage of all the health-related information along with wearables devices creates a data silo that can be used to provide better care and cut costs associated with operating a care facility. **Including all the data from different care providers, personal health records, wellness apps makes a comprehensive pool of information that is greater than a sum of its parts.**
- All of the information gives an insight on the customer's history and, current state analysis and can be used to make a prognosis of conditions. That means all the raw data analyzed in a proper way can help detect health issues before they are critical — and make suggestions

The future:

- AI algorithm to make preliminary diagnosis and predict health conditions before they happen — based on data provided.
- Interface for customers and companies to interact with the data transfer and serves as a singular data silo for the all-round digital persona. Emergency services can access data and patient records.
- Data researchers are presented with a toolbox to purchase data based on explicit consent and rewards to data owners. All of this while customers maintain complete control over their private dat

Solution

Healthcare and insurance

- Healthcare plans, medical prescriptions, and drug accounts can be tokenized in a unified registry- accessible to everyone: other doctors insurance companies.
- With help of blockchain technology, unauthorized change, access and use of citizens' data becomes impossible, because any information of these actions is recorded in the system.

Worldwide experience

- In 2016, Netherlands-based company Prescrypt in collaboration with SNS Bank NV and Deloitte developed a blockchain-based app that makes medical services more accessible for chronic patients.
- In the first half of 2016, the Estonian government agreed with company, Guardtime to transfer data of more than 1 million state citizens' medical cards to blockchain database.
- In 2016, USA-based startup BitHealth began to use blockchain to give their patients additional payment opportunities with their insurance companies

The GIG economy is on the rise

GIG-economy worldwide

$500B+

- Self-employed, on-demand workers (i.e. Uber or AirBNB independent contractors)
- 25%-35% expected annual growth over the next 5-7 years
- gigs are sitting in 14K+ co-working spaces globally (2020)

GIGs

57M

freelancers exist in the US, nearly 40% of the workforce.

$1.3T was contributed to the US economy by freelancers in 2017.

ONCE AGAIN: BORDERLESS APPROACH IS STILL VERY NEW FOR BANKS (AND REGULATORS)

TC

Startups
Apps
Gadgets
Events
Videos
—
Crunchbase
More

Search

Apple
Artificial Intelligence
TechCrunch Tel Aviv
Cryptocurrency

Login / Sign up

Stripe Expands Startup Tools With Atlas, For Foreign Companies To Incorporate In Delaware

Ingrid Lunden @ingridlunden / Feb 24, 2016

Comment

Stripe today took a big step ahead in its bid to offer more tools for startups, beyond the basic payment services it already provides. The company today unveiled Atlas, a platform to let startups incorporate more easily in the U.S., specifically in Delaware with services that include incorporation, share issuance, adding directors, setting up bank accounts and (of course) **Stripe** payment accounts.

Atlas — which launches today as an invite-only beta, was announced today by Patrick Collison, co-founder and CEO of the company, on stage at MWC in Barcelona.

Atlas will start with U.S. incorporation but will over time provide "more hubs" so that businesses can incorporate wherever it "makes sense for them to register," Collison said.

Bank like a local with Transferwise's new 'borderless' debit card that gives you a free account anywhere in the EU, Australia, the US and Britain

- New debit card which includes bank accounts for several different countries
- Transferwise says its new account is eight times cheaper than a traditional bank
- It's free to transfer more than 40 currencies within the account
- You'll have to pay a small fee for withdrawing cash in a different currency

By REBECCA GOODMAN FOR THISISMONEY.CO.UK
PUBLISHED: 08:37 BST, 7 May 2018 | **UPDATED:** 15:12 BST, 7 May 2018

Share 89 shares 18 View comments

A 'borderless' debit card has launched that gives people the chance to operate a bank account in several different countries around the world.

It is aimed at those travelling, living and working abroad to give them more flexibility when spending and sending money and to lower their overall costs.

It's been launched by Transferwise, which claims it's the first multi-country account and debit card.

This is Money has taken a closer look to see just how it works, who it suits and how the prices compare.

Search
All Articles Share prices
Portfolio Newsletter Guides
Savings rates Deals Calculators

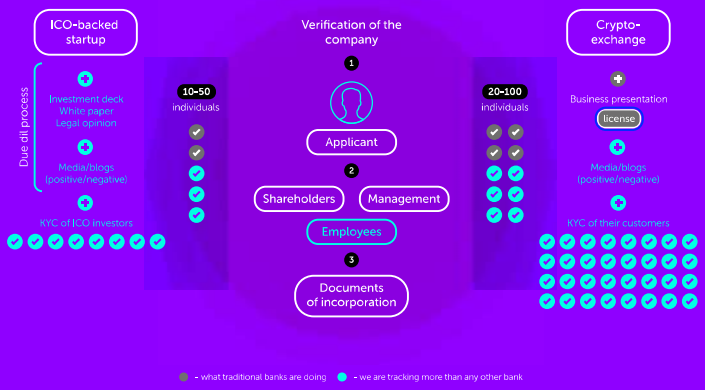
THIS IS MONEY PODCAST
What on earth has been going on in Italy and what does it mean for you? Listen to the This is Money podcast

BORDERLESS APPROACH DEPENDS ON UNIFIED KYC AND AML

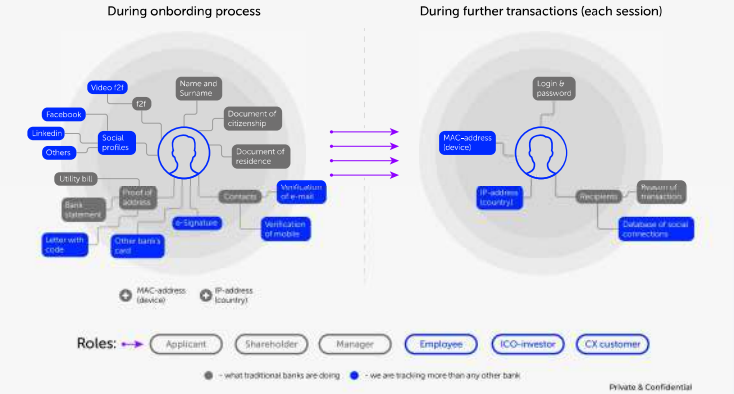
AID

Arival developed and integrated a high-standard compliance policy, based on digital and **technologically advanced KYC and AML** processes, in order to fully comply with the world's most severe regulatory requirements, demanded by **US' Federal Reserve Bank.**

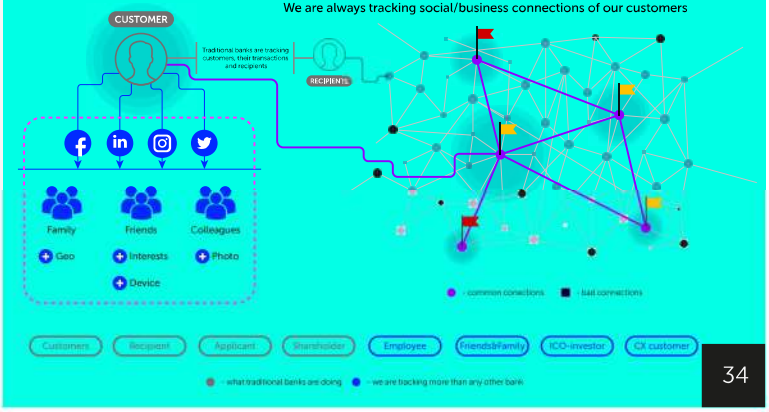
KYC: we really understand our business-clients



KYC (Each business as a group of people)

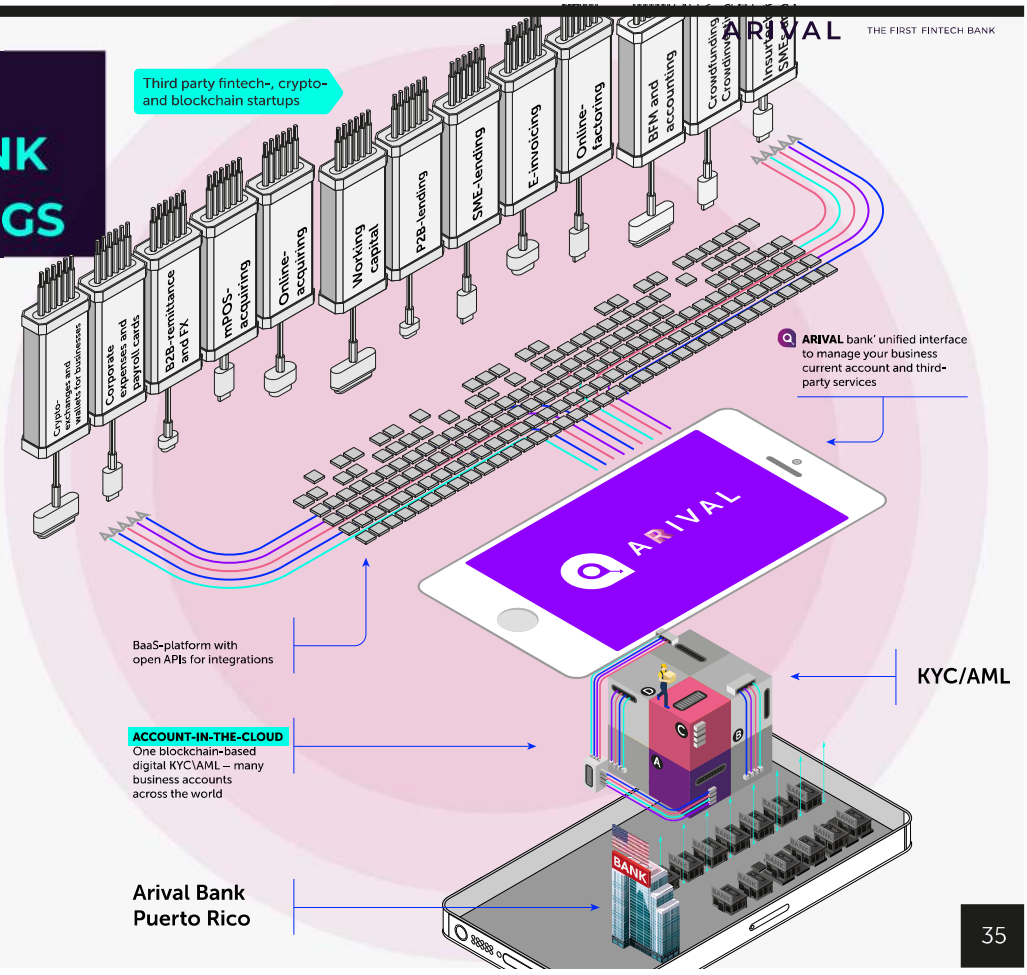


You are who your friends are



ARIVAL BANK: BORDERLESS BANK FOR SMES AND GIGS

- Digital Banking meets Fintech
- Tech-forward banking platform: open API to easily integrate 3rd party fintech products & services
- US-based banking license
- **We only work with fiat currency -** just like any other traditional bank
- Our digital KYC/AML process is sophisticated, meticulous, and designed for crypto-related SMEs



Puerto Rico is the gateway to the US market

WHERE IS THE ~~CRYPTO~~ BLOCKCHAIN CAPITAL OF THE US?

POWERTO R ICO

Blockchain {$powered; territory'//>

If you want to know more – you can download our research: https://goo.gl/AV7Ycx

- As cryptocurrency becomes more and more viable, states like Wyoming, California, Delaware, Tennessee and Arizona are racing to pass cryptocurrency-friendly legislation in an effort to become the blockchain capital of the country.
- Puerto Rico became part of the United States following the Spanish American War in 1898, with Commonwealth status introduced in 1952. The residents of Puerto Rico are, therefore, citizens of the United States. There is no Central Bank in Puerto Rico, it is the US Federal Reserve Bank which acts as a Central Bank. Banks are insured by the Federal Deposit Insurance Corporation (FDIC). They are subject to all Federal controls applicable to banks in the United States of America. Banks in Puerto Rico are part of the U.S. banking system with a few differences in tax laws.
- The fintech sector is a natural fit for Puerto Rico's entrepreneurs and for the island's economic and industrial reawakening. Compared to manufacturing, healthcare or other industries, fintech businesses are relatively easy to start and many can operate anywhere with a stable internet connection and remote server access.
- Puerto Rico offers an unparalleled tax incentive: no federal personal income taxes, no capital gains tax and favorable business taxes.
- Puerto Rico's Act 20 and Act 22 make the island an attractive place for fintech investment. This initiative allows investors who establish a residence in Puerto Rico a low-tax alternative for doing business.

Compliance Demystified: A Beginner's Guide

8 min read · Mar 25, 2024

Slava Solodkiy

In today's fast-paced digital world, where every transaction leaves a digital footprint, the importance of compliance can't be overstated. But what exactly is compliance, and why does it matter to your business? At its core, compliance involves a series of steps and checks designed to ensure businesses operate within legal and regulatory frameworks. This not only applies to financial institutions but any business that deals with customer data.

In a rapidly evolving digital landscape, understanding the intricacies of compliance has never been more critical. Compliance is an extensive field that encompasses various practices and procedures aimed at ensuring businesses and individuals adhere to regulatory standards and prevent illicit activities. Here's a deep dive into the multifaceted world of compliance, simplified for beginners.

Here are the 7 main essentials:

1. **CDD** (customer due diligence) or Onboarding: The process of collecting and evaluating customer information during the onboarding process — including:

- **KYC —** know-your-customer (and know-your-employee, know-your-passenger, etc),
- **KYB —** know-your-business (plus, **UBO**s, ultimate beneficial owners, and executives here are subject of KYCs too)
- KYCC (know your customers' customers) — for **FI**s (financial institutions), especially BaaS and correspondent banks
- risk identification in compliance involves categorizing clients based on their geographic location, industry, and other factors that may elevate their **risk profile**

2. **EDD** (enhanced due diligence — **RFI**s, requests for information: any additional information, documents and evidences: additional, mostly manual as for today, questions to understand reasons or nature of action)

- if\when high risk customer (or if **SAR —** suspicious activity report)
- **high risk:** by geography (Russia, etc) or by industry (crypto, cannabis, etc)
- a critical step that involves verifying the identity of your customers and to prevent fraud is '**source of funds, source of wealth**'
- 'source of transaction': it's about constantly comparing the information received during onboarding with ongoing transactions to spot anything out of the ordinary.

3. Ongoing compliance, or **AML** (anti money laundering) and transactional monitoring (80% of compliance crime could be catched only during EDD and ongoing compliance, real ML-specialists are smart enough to pass any onboarding requirements,

- but *value here is to create CDD on such level to make further investigation faster and better "**trackable**"). **Compliance is about better management of your risks**, rather than an unrealistic attempt to create an ideal system to recognize good and bad persons, and good and bad transactions.*
- permanent comparison between, first, information received during onboarding about ***Sender***, second, current ingoing\outgoing ***transaction*** (amount, currency, ***reason***), and third, about ***Recipient***

- requirement to ***re-verify all answers and documents provided during onboarding*** (expired, changed, blacklisted): monthly, quarterly, annual, every 2–3–5 years

- (part of EDD regarding AML) **SAR** (suspicious activity report, mostly for FinCEN) — new (changed) information about onboarded person or company, suspicious transaction by quality (reason for transaction or recipient) or quantity analysis (size or amount of transactions)

4. CCO, Chief Compliance Officer (and Compliance team: onboarding, EDD, AML specialists) — behind every compliance framework is a team led by the Chief Compliance Officer, tasked with ensuring the organization stays on the right side of regulations.

5. Compliance Policies (documents about possible clients, potential risks and risk covenants, rules and procedures regarding onboarding, SARs, **offboarding** and "*data cemetery*")

- **Risk segmentation** (of potential clients)

6. Compliance education (of everyone within the company related with potential compliance risks)

7. Compliance audit (could be internal, but better — external)

Nansen.ID, for instance, focuses on streamlining the CDD process, with plans to expand into KYB, KYCC, and more sophisticated monitoring solutions. It's a testament to the evolving nature of compliance solutions, leveraging technology to make due diligence faster, more accurate, and less intrusive.

In the context of compliance, identity verification goes beyond just knowing who someone is. It encompasses everything from biometric data (like fingerprints or retina scans) to documents and even social connections. The challenge is to **create a**

system flexible enough to accommodate the diverse ways identity can be established and verified.

Rather than viewing **compliance as a necessary evil, forward-thinking companies see it as an opportunity** to build trust with their customers and differentiate themselves in the market. By managing risks effectively, they not only avoid penalties but also enhance their reputation and customer loyalty.

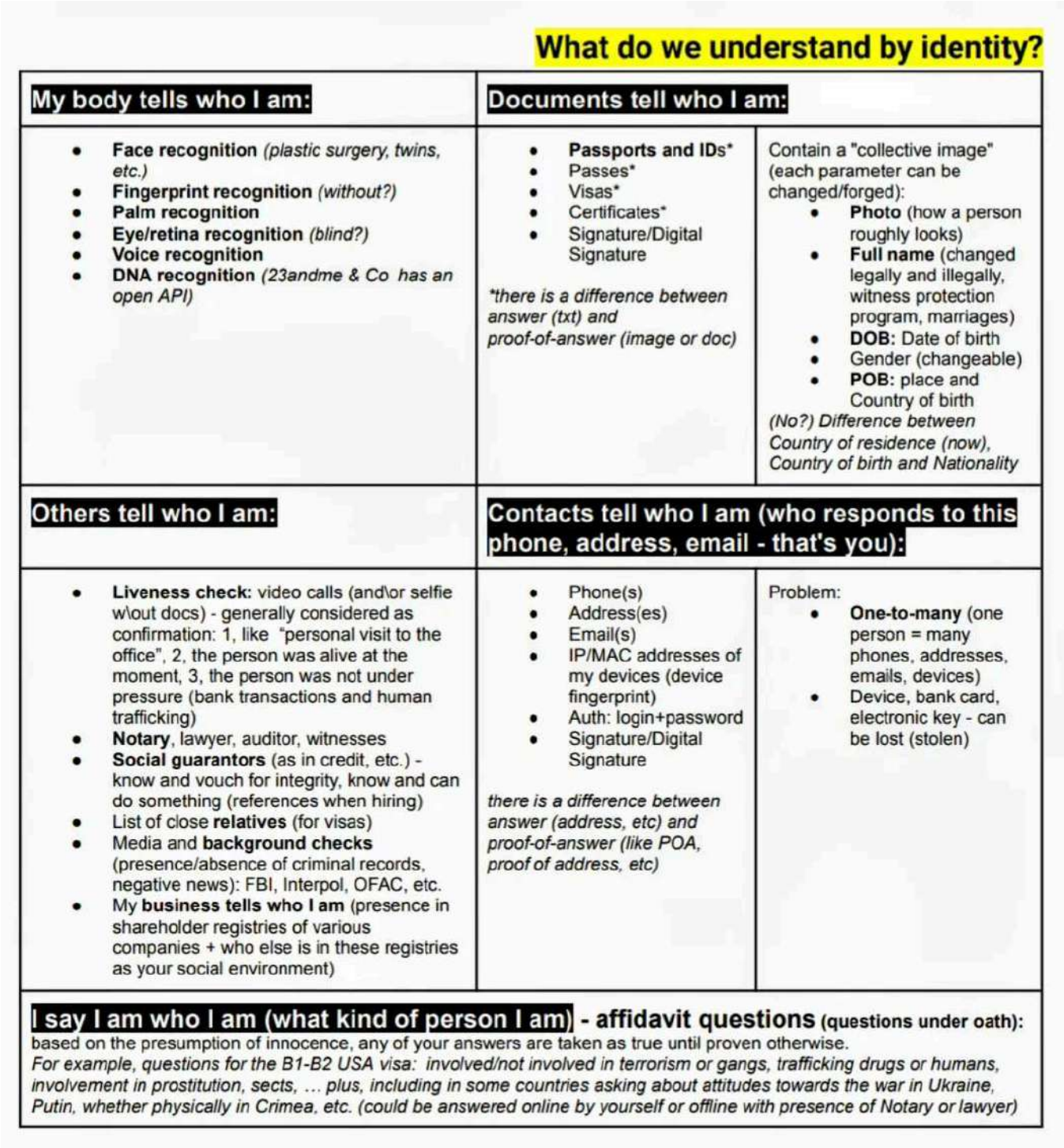
How could World ID be better? Or at least useful

World ID from Worldcoin and Tools for Humanity is currently an absolutely useless thing - no one can answer the simple...

www.linkedin.com

KYC: The Multifaceted Nature of Who We Are in the Digital World

In the ever-evolving digital landscape, the concept of “digital identity” has become increasingly complex. It’s not just about who we are online, but how various elements come together to create a unique digital persona. Let’s delve into the different aspects that constitute our digital identity:



'Truth' often depends on the Hypothesis, which dictates your risk tolerance

1. **Physical Attributes: The Biological Passport (My body says who I am)**

- Facial Recognition: While highly popular, it's not foolproof. Changes in appearance, plastic surgery, or having a twin can affect its accuracy.
- Fingerprint Recognition: Not everyone has discernible fingerprints, posing a challenge.
- Eye/Retina Recognition: This method excludes individuals without sight.
- Voice Recognition: Ineffective for those who are mute.

- DNA Recognition: Although unique to each individual, privacy concerns and ethical implications come into play, especially with open API platforms like 23andMe.

2. Documented Identity: The Paper Trail (Documents say who I am)

- Our identity is often tied to official documents: Passports, visas, and various certifications.
- These documents provide a "collective image" including (potentially changeable) parameters like name, date of birth, gender, and nationality. (Media and background checks, presence/absence of criminal records, negative news: FBI, Interpol, OFAC, etc.)
- Signatures, both physical and\or digital.

3. Social Endorsements: Our Community's Voice (Others say who I am)

- Social guarantors (akin to credit references), vouch for an individual's character or skills (employment references).
- Legal professionals like notaries, lawyers, witnesses, lay judges and auditors also play a role in certifying identity (and they need to verify you too).
- List of closest relatives (for visas),
- Media and background checks (presence/absence of criminal records, negative news): FBI, Interpol, OFAC, etc.
- My business says who I am (presence in shareholder registers of different companies, plus who else is in those registers as your social environment).

4. Digital Footprint: The Tech Trace (Contacts say who I am: who responds to this phone, address, email — that's me)

- Contact details like phone numbers, email addresses, and physical addresses.
- The digital fingerprint of our devices (IP/MAC addresses).
- Knowledge of login credentials.

- Challenges include the "one-to-many" nature (one person having multiple emails, phones, etc.) and the potential for device or key loss.

5. Personal Affirmation: The Self-Declaration (I say who I am, and what kind of person I am)

- Affidavit-style questions under oath assume truthfulness until proven otherwise, covering a wide range of personal history and beliefs.
- Video calls are becoming a standard for identity verification (and liveness check), offering real-time interaction and ensuring the person's immediate presence and freedom from coercion.

In this era, digital identity is a patchwork of biological traits, documented evidence, social endorsements, digital footprints, and personal affirmations. As technology evolves, so does the complexity of identifying and verifying an individual in the digital space. The challenge for businesses and regulatory bodies is to navigate this complexity while ensuring security, privacy, and ease of use for individuals. The future of digital identity lies in finding a balance between technological advancement and ethical considerations, shaping how we define ourselves in the digital world.

Diverse Use Cases of Compliance Across Industries

1. **Banking.** Opening a bank or insurance account goes beyond just knowing who you are. It's about ensuring you're not involved in money laundering, tracing the origins of your funds, and understanding the purpose of your transactions. Requirements include basic personal details, professional background, guarantors, and accounts in other banks or tax statements. This is accompanied by background checks, transaction monitoring, and regular audits.

2. **Telecommunications.** When issuing SIM cards, there's a need to mitigate security risks by identifying who, when, and where a SIM card was activated. Basic personal information and identification are required.

3. **Healthcare.** Booking a doctor's appointment or undergoing medical tests requires identifying both the patient and the doctor, along with consent for the collection, processing, and storage of biological material.

4. **Housing.** Renting a property involves risk hedging (financial stability) and ensuring the safety of other residents. This involves basic queries and credit ratings. For purchases, the source of funds is often scrutinized.

5. **Education.** Admissions to schools or universities entail security considerations. This includes verifying personal details, employment and education history, social references, and sometimes additional details like race, religion, or veteran status in certain countries.

6. **Employment.** Employment requires comprehensive identity verification, including past employment and education, social references, family affiliations with government bodies, criminal history, and willingness for background checks and drug tests. Hiring a nanny, driver, or cleaner also demands identity verification to ensure safety and trustworthiness.

7. **Visa Issuance.** Visa services like VFS Global and TSL Contact collect and transfer applicant information to embassies, covering family background, travel history, financial stability, and affidavit questions. But all this information is absolutely non-reusable at the moment — every time you fill out the same forms and answer the same questions.

8. **Airport and Hotel Check-ins.** Airlines verify if a passenger is wanted or poses a security threat, while border controls confirm the individual's entry. Hotels ensure guest safety by requiring personal details and passport copies.

9. **Online and Offline Services:** Dating services (Tinder, Bumble, etc), Airbnb, Uber, and **age-restricted services** all require identity verification for safety and legal compliance.

10. **Marriage and Divorce:** Verification of individuals in marriages and divorces, including presence of a third verifier and legal jurisdiction, is crucial.

11. **Legal Agreements and Arbitration:** Notarization of agreements and arbitration involves verifying the parties involved, the witnesses, and the terms agreed upon.
12. **Business Formation:** Company creation requires verification of each shareholder, director, and employee.
13. **Wills and Estates:** Verification of the testator, executor, beneficiaries, asset list, and jurisdictional considerations are key.

The implementation of compliance spans across various sectors, each with its unique requirements and challenges. From personal to professional, transactional to legal, the digital identity serves as a crucial tool for verification, security, and trust in our interconnected world.

The pivotal role of compliance in the realm of digital identity is often overlooked. For any identity system to truly come to life, it must first be accepted. This acceptance is not just about technology adoption but involves navigating regulatory landscapes and understanding the end-user experience. Without this, the most innovative digital identity solution remains inert.

Compliance is an integral part of doing business in today's global economy. By understanding its components and staying ahead of regulatory changes, companies can navigate the complexities of the modern market with confidence. As solutions like Nansen ID demonstrate, technology plays a crucial role in simplifying compliance, making it more accessible for businesses of all sizes.

Identity verification is a cornerstone of compliance, encompassing everything from biometric data to official documents like passports and IDs. The goal is to create a comprehensive profile of a client, incorporating various aspects of their identity, activities, and affiliations. Today's digital world presents new challenges and opportunities for compliance. With technologies like blockchain, digital banking,

and online platforms expanding rapidly, compliance frameworks must adapt to ensure security, privacy, and adherence to regulatory standards across all digital transactions.

I initially invested in and advised the KYC startup **BASIS ID** (which has since been acquired and is now under ZignSec) and **A.ID**, a compliance-as-a-service company (also acquired). Four years back, as the founder and CEO, I set up Arival Bank (arrival of a rival), a compliance-centric fintech. **ArivalBank.com** serves as a digital bank catering to high-risk international clients under a US banking license. Owing to its compliance milestones, Arival is included in the FinCEN innovation group.

Kyc Aml Compliance Kyb Fintech

Edit profile

Written by Slava Solodkiy

954 followers · 244 following

chief believer x linkedin.com/in/vsolodkiy

From Dissident to Detective: On the Way to ShmagunGPT

16 min read · Mar 26, 2024

Slava Solodkiy

OSINT Skills Made Alexey Navalny and His Team Popular

It was the skills in Open Source Intelligence (OSINT) that helped Alexey Navalny and his team gain popularity. Most of his AML and anti-corruption investigations were based on open data. One of their most striking investigations, "He Is Not Dimon to You," has garnered 46 million views. It details how friends, classmates, and trusted persons of Dmitry Medvedev own non-profit organizations that receive generous donations from oligarchs and state loans. The investigation triggered protests across Russia, and online shopping orders helped prove the connection between Medvedev and the man registered as the owner of his non-profit organizations. Shirts and sneakers ordered under the name and address of the formal owner eventually ended up with Medvedev, who appeared in them publicly without issue.

EU on easing the opening of bank accounts for anti-Putins

EU lawmakers on easing the opening of bank accounts and obtaining visas for Russian opposition

medium.com

Their investigations have often put them at odds with powerful state actors, leading to legal challenges and personal risks. The work of Grozev, Shmagun, and Dobrokhotov exemplifies the critical role of investigative journalism in uncovering truth and holding the powerful to account. And regarding **compliance, KYC, and**

AML — I would recommend regulators, banks, and fintechs to learn from them (as the CIA does), rather than from conferences and office research by major consulting firms.

Christo Grozev, Olesya Shmagun, and Roman Dobrokhotov are well-known investigative journalists and researchers renowned for their work in **exposing various illicit activities, money laundering** and government malfeasance, often involving high-profile cases and sensitive political matters.

Christo Grozev is known for his association with **Bellingcat**, an international collective of researchers, investigators, and citizen journalists that uses open-source and social media investigation. Grozev has been instrumental in investigations into the poisoning of Sergei Skripal and Alexei Navalny, the downing of Malaysian Airlines flight MH17, and other notable cases involving Russia.

Like Grozev, Olesya Shmagun has contributed to uncovering corrupt practices and AML. Her work, much like that of her peers, involves meticulous research and the use of open-source intelligence (OSINT) techniques.

Roman Dobrokhotov is the editor-in-chief of The Insider, known for his involvement in major investigative efforts alongside Bellingcat. Dobrokhotov has faced significant legal and political pressure within Russia, including police raids and being targeted by defamation lawsuits, as a result of his investigative work. His efforts have contributed to revealing the actions of Russian intelligence and military services in various international incidents.

Roman Dobrokhotov (read the full article on Wired) has become a notable figure in exposing the clandestine operations of Moscow's GRU military intelligence agency. Dobrokhotov's journey from a protester challenging Kremlin narratives to a fearless investigative journalist is marked by his crucial role in uncovering the identities and activities of Russia's most covert military spies and assassins, including their involvement in high-profile cases like the attempted assassination of Sergei Skripal with a nerve agent. Dobrokhotov's work not only exemplifies journalistic bravery but also underscores the vital importance of independent OSINT-media in challenging state-sponsored narratives and uncovering the truth via 'follow the money' approach.

Recently, Grozev, who won an Oscar for the documentary film about Navalny, has been focused (together with Dobrokhotov) on investigating the activities of Jan Marsalek from Wirecard and is preparing a documentary film about him. Following the unexpected death of Navalny, Christo has temporarily concentrated, along with other independent investigators, on collecting and analyzing data related to the death of the opposition figure, known for his investigations into corruption and money laundering, and those involved in it.

A most wanted man: Fugitive Wirecard COO Jan Marsalek exposed as decade-long GRU spy

Fugitive Wirecard COO Jan Marsalek wasn't just responsible for Germany's largest financial fraud in history. He was...

theins.ru

Hristo Grozev is a Bulgarian investigative journalist, media expert, and media investor, leading investigator at The Insider, previously worked with Bellingcat. He is one of the main authors of the investigation into the involvement of FSB Russia employees in the poisoning of Alexey Navalny. Winner of the European Press Prize and the Emmy Award for his investigative journalism. Around 2014, he started investigative journalism with Bellingcat: "I'm doing something I'm good at, finding things others miss, using my knowledge of Russia, the neighboring countries, including Ukraine, working with people in these countries, and being concerned about their governments (both in Russia and Ukraine) deceiving citizens. I do this voluntarily, spending my own funds on investigations."

In 2019, Grozev (together with Roman Dobrokhotov and Daniel Romein) was awarded the European Press Prize for Investigative Journalism & London Press Club Prize for Digital Journalism. In 2021, Bellingcat and CNN received an Emmy Award in the category of “Outstanding Investigative Report in News” for Hristo Grozev’s investigation. They also made reports against NATO, which was illegally selling weapons to Saudi Arabia for the civil war in Yemen, did analysis of Turkish and Greek crimes during the migrant crisis. Grozev was accused of organizing the escape abroad of journalist Roman Dobrokhotov.

Grozev lived in Vienna for 20 years until 2023, where he was under police protection due to his exposes about Russia. In February 2023, he stated that he moved to the USA after Austrian authorities told him they could no longer guarantee his safety. In August 2020, Grozev stated in an interview with Deutsche Welle that the poisoning of Alexey Navalny was similar to the attempts on Emelyan Gebrev and Sergei Skripal, in which Russian special services are suspected.

Responding to a question about informants, Grozev said: “We work only with sources who understand the risk they are taking.” He also denied any connection with the CIA, noting that Western intelligence had not even reached the information published by independent journalists. Grozev has bet on crowdsourcing: now anyone can join the work of investigative journalists, comparing data from flight tables with information about the time and place of high-profile poisonings and strange deaths. Several matches were immediately found.

Olesya Shmagun (Princeton, previously graduated from the Faculty of Journalism at Moscow State University in 2012, continued her studies in graduate school) — Pulitzer Prize winner for the investigation of the Panama Papers, co-founder of the publication “Important Stories”, employee of the Center for the Study of Corruption and Organized Crime (OCCRP), four-time winner of the monthly journalism prize “Redkollegiya”. In April 2017, as part of the International Consortium of Investigative Journalists along with 300 other journalists, received the Pulitzer Prize in the category for explanatory journalism for the investigation into the “Panama archive”. In 2023, she graduated from the Woodrow Wilson School of Public and International Affairs at Princeton University, earning a master’s degree in public policy.

Recently, Olesya and I were chatting about Nansen.ID and… ShmagunGPT, and I really think a tool for Enhanced Due Diligence (EDD), inspired by Olesya’s investigative magic, is exactly what we need, especially in the worlds of banking and fintech. I threw an idea at Olesya about creating a digital identity solution for opposition figures or maybe even a digital bank for those in exile… With Olesya’s incredible knack for digging into money laundering schemes, imagine digitizing her expertise to become a nemesis for money launderers everywhere with something like ShmagunGPT.

Nansen ID

NANSEN.ID is a digital identity solution designed for opposition members and political emigrants from sanctioned...

www.nansen.id

I dream of Nansen.ID as a business with a heart, channeling profits into the hands-on investigative work of journalists like Olesya, Christo, and Roman. Their investigative work provides insanely useful data for compliance in banks and fintechs — at the very least.

From a regulator’s perspective, **KYC is less about knowing your customer and more about understanding where their money’s from, how they got it, and where it’s headed**. I’ve been around the block with bank compliance, and Olesya’s battled against the baddies, uncovering corruption and laundering schemes. We’re basically **enriching traditional data with fresh, unconventional insights**. Plus, imagine if we

built a backend sort of like ShmagunGPT, **training a neural network based on Olesya's investigative methods**. It'd be like an automated sidekick for other investigators and compliance officers.

Filling out the same personal info over and over for every new bank account, insurance policy, mobile plan, flight, hotel stay, apartment lease, and more — isn't it exhausting? That's where the last bit about "convenience" comes in (i.e., no need to re-answer if you've already addressed a question; digital ID will auto-fill the existing answer). That's for the end users.

For banks and other entities, it's crucial to grasp that the slickest KYC process at onboarding won't shield you from fraud and scammers: only 20% get caught at the get-go, while the other **80% are nabbed based on their transactions later on. To catch these guys later, you need to "cast a net" at onboarding** so that any anomalies in behavior can be spotted more swiftly, allowing a quick rewind to pinpoint accomplices. The **real slick criminals layer their operations with legit transactions by innocent folks — no system will red-flag them at onboarding**. But setting up the system to notice oddities sooner or swiftly backtrack to find connections? Totally doable.

Banks, fintechs, and insurers pay for this. But who really benefits? End users!, especially those who've been denied accounts or visas. It's a boon for the whole regulatory ecosystem, from visa centers and telecoms to hotels and airlines, even extending to online election services. In essence, it's a trade-off:

1, I get that my nationality (or additionally, my industry affiliation) blocks me from certain benefits and creates hurdles I'd rather not have; I want to enjoy those benefits.

2, I know you don't see me as the bad guy; you're just covering your bases because you can't tell us apart. So, my "payment" is becoming more open and transparent with you.

3, You accept this “payment,” allowing you a closer look into my life, with the agreement that if someone linked to me steps out of line, they get cut off from the network of benefits.

It’s a way of saying, “I’m cool, let me in,” while also ensuring everyone plays by the rules. As in Ancient Greece: **exile from the polis** (“collective responsibility” in action) as the main possible “punishment”.

The CIA has announced a new strategy for working with open-source information, aiming to expand and enhance the collection and analysis of data amidst the ever-growing information stream. The document, presented by the Office of the Director of National Intelligence (ODNI) and the CIA, discusses the development of methods for collecting, creating, and delivering intelligence from open sources (OSINT) until 2026. Special attention is given to the potential of artificial intelligence and machine learning in improving the processing of open data, as well as the risks associated with verifying the authenticity and reliability of information.

As part of the strategy, ODNI has enlisted leading cybersecurity expert Jason Barrett to implement key directions. His task is to integrate innovations into OSINT work based on the CIA’s experience in this field over the last year. The CIA has also developed AI technology, similar to ChatGPT, for selecting relevant information from the vast amount of available data. This new tool automates the OSINT processing workflow, highlighting key data for analysis. Senator Mark Warner, the chair of the U.S. Senate Intelligence Committee, emphasized the importance of such tools, noting that the traditional view of prioritizing covert information collection is giving way to the recognition of the importance and effectiveness of using open data.

Open Source Intelligence (OSINT) involves searching and analyzing public information to ultimately gain new knowledge. Essentially, OSINT investigators primarily work with data that has already been published by someone at some point. States and corporations possess a vast amount of information, part of which can be found online or obtained upon request. However, the path to this data often lies through websites that are invisible to search engines, through cumbersome databases, little-known archives, and clunky interfaces. The investigator's skill lies in finding information, analyzing it, and making it understandable to a broad audience.

OSINT emerged in the 20th century as a military technology. One of the first entities specialized in such investigations was the Research and Analysis Branch of the American Office of Strategic Services, the precursor to the CIA. Today, open-source data intelligence methods are used by intelligence and government employees, as well as professional investigators and journalists.

OSINT primarily involves working with open data, but investigative teams sometimes use non-public sources. For instance, the investigations into the poisonings of Alexey Navalny or Sergei and Yulia Skripal are based on mobile operators' billing data (information about incoming and outgoing calls, SMS, internet traffic), passenger lists of trains and airplanes, leaked databases of commercial companies, and other data. Such information can be purchased on Telegram channels or in the darknet.

Other open services used by OSINT investigators can be divided into groups:

- **Maps and satellite images**, not only the popular Google or Yandex but also Bing and OpenStreetMap (OSM). The latter operates on a Wikipedia-like principle — users can add and mark objects on the map themselves. For OSM, there's also the Overpass-turbo app, allowing for the download of coordinates for specific objects on the map, like all stores of a certain retail chain or all drinking water fountains in a city.
- **Services that allow searching by photo**, known not only to investigators but also to ordinary people. You upload a photo of a person, and the site shows you their

social media page, and sometimes even friends they preferred to hide. Many of these platforms are paid but have limited free functionality, such as PimEyes or Search4Faces. There are also services providing information by phone number or car license plate.

- Commercial **company registries** reveal the company's founding date, authorized capital, legal address, and people associated with it.
- **Vehicle movement services.** The popular site Flightradar collects flight numbers, information about the starting and ending points of routes, registration number, country of registration, and other data about all flights. Similar services exist for tracking sea vessels.
- Services for **searching removed information.** Resources like WaybackMachine allow you to find and view old versions of websites — in case they have stopped working or their data has been removed.
- **Metadata analysis** systems can extract information from files of various formats about the date, time, and device that created a specific document. Or collect information about entire websites — when and by whom a domain was registered and which other domains are associated with that site. Services like who.is and Domain Tools allow for this.

For example, In "OSINT Techniques for Sensitive Documents That Have Escaped Into The Clear Web," Christina Lekati highlights a common vulnerability among organizations: sensitive documents inadvertently exposed online. Lekati notes that participants frequently discover documents posing significant risks to their organizations on the clear web, often due to employee errors or oversight. She emphasizes the importance of proactive searches to identify and manage these documents before they're exploited by threat actors. The article offers a tutorial on advanced search queries, using special characters and operators to refine searches for specific documents related to an organization. Lekati provides practical advice on how to use Google Dorking, a technique that utilizes special search strings to find sensitive information efficiently. Highlighting the potential goldmine of information that documents like contracts, internal processes, and admin credentials can represent, she warns of the exposure risk to competitors, the media, and other entities. To combat this, Lekati suggests several ready-to-use search queries involving operators that focus on finding specific file types, such as PDFs, PowerPoints, and Excel files. She encourages creativity in conducting OSINT checks

and underscores the ease of mitigating such risks by eliminating or managing the exposure of sensitive documents. She advocates for OSINT as a defensive discipline, crucial for organizations to act proactively against potential security breaches.

In 2015, 13-year-old Justin created a Twitter account under the nickname Intel Crab and invented a fake persona of a teenager from Donetsk. He collected videos, photographs, and quotes from people in the war-torn Donbas to post on his account. When Justin realized he had become popular — with thousands of followers — he stopped pretending to be a boy from Donetsk.

Justin decided to take a more serious approach. He began analyzing and verifying the information he gathered, as well as recreating context with additional tools like plane tracking services and satellite images. Now 20 years old, Justin regularly finds photos and videos from event locations, opens maps, and checks whether the specified geolocation matches what is visible in the images. He publishes his findings, for example, tracking changes in the amount of equipment at Russian military bases using satellite images, and monitored photos posted by Kadyrovites in Zaporizhzhia on VKontakte and Telegram, publishing their locations. Justin now has nearly 309,000 followers. This year, he is graduating from the University of Alabama and saving money to go to Ukraine to see the country not just on a monitor screen.

Perhaps **the most famous open-source investigation team is Bellingcat.** Its founder, Elliot Higgins, has been writing about the use of banned weapons and violations of humanitarian law in Syria since 2012 on the Brown Moses Blog. In 2014, he assembled a team and began investigating war crimes in Ukraine.

One of Bellingcat's most notable works is the investigation of the downing of Malaysia Airlines flight MH17 in Donetsk Oblast in July 2014. Journalists established that the missile that downed the plane was Russian and launched from territory controlled by Russian authorities. Using photos and videos by eyewitnesses who captured the Buk missile system in various locations, investigators tracked its movement from Russia to Ukraine. They reconstructed its route thanks to a cargo platform photographed in various places in Russia and Ukraine. Initially, the platform carrying the system had four Buk missiles, but the day after the plane's downing, only three were visible, and it was headed back towards Russia. Even the shadows cast by objects in photos and videos were important — using the SunCalc program, journalists calculated the approximate time of filming. Another

significant detail was the smoke trail left by the missile. Using it, Bellingcat identified the missile's launch site on satellite images and eyewitness recordings.

The MH17 case brought popularity to both Bellingcat and the OSINT method itself. Media began to reference data from investigative teams more frequently, and some newsrooms established their own data and OSINT departments. The spread of the internet **allowed OSINT methods to extend beyond military intelligence and the professional community of investigators**, becoming a new form of digital activism.

Artificial intelligence could prevent errors and inaccuracies caused by the human factor. OSINT blogs constantly write that potentially AI could be delegated several tasks at once, such as determining the location of a shot or distinguishing between tanks and IFVs in satellite images. However, current software still struggles with this task. The military uses more advanced AI developments: their algorithms can recognize enemy troops in satellite images, predict the course of hypersonic missiles, and even autonomously attack enemy targets. (Read about how artificial intelligence learned to wage war.)

However, investigators can indeed have an impact on the world. The **results of work based on open data are sometimes considered by courts.** In 2018, the prosecutor of the International Criminal Court (ICC) issued an arrest warrant for Libyan General Mahmoud Werfalli, who carried out public executions. The ICC based its evidence on the analysis and geolocations done by the Bellingcat team. The Hague Court, which considered the case of the MH17 crash in Ukraine, also cited materials from Bellingcat investigations. The International Investigative Group on War Crimes in Ukraine, initiated by Eurojust, requested materials from a joint investigation by "Important Stories", OCCRP, and Der Spiegel on the supply of microelectronics and drones to Russia bypassing sanctions.

However, **investigators want their findings to be used more actively.** The Conflict Intelligence Team is currently working with other investigative projects to propose amendments to the legislation of EU and US countries. Investigators want their conclusions to have greater value in crime investigations. Only those who are inconvenienced by these investigations express outright distrust of OSINT researchers' materials.

The barrier to entry in OSINT is low — only internet access and free time are needed. No special education is required — there is no university or training

program to graduate from and receive a diploma as an **OSINT investigator (although private courses are available**). Investigators themselves say that the main qualities needed for this work are patience and attentiveness. “90% of the time, we sift through a huge amount of material, photos, and videos. It’s very tedious and hard work,” says Ruslan Leviev in an interview with Kit.

If you’re already engaged in cyber investigations or want to gain knowledge in this field, I recommend applying for the GIJN’s free online course (I’ve already applied). The course topics include: Basics of Digital Investigations, Threat Landscape: Malicious and Spyware, DNS: Websites and Infrastructure, Investigating Disinformation and Trolling, Network Analysis. Instructors: Craig Silverman, ProPublica reporter; Jane Lytvynenko, independent journalist (Guardian, BuzzFeed News, Joan Shorenstein Center at Harvard); Etienne “tek” Maynier, Amnesty Tech Lab staff; Luis Assardo, Reporters Without Borders staff and independent researcher. The course starts on April 29 and will run every Monday and Thursday for 6 weeks.

We review and practice other popular OSINT tools:

- **Maigret** is an innovative tool designed for data analysis from various social platforms. It offers extensive capabilities for information gathering, user activity analysis, connection finding, and other functions. This tool has flexible settings for data collection and analysis, allowing you to choose social networks and save results into files. Maigret supports over 3000 sites for username searches. An excellent tool for username searches, it’s maximally simple to install and equally easy to use.

- **Mr.Holmes** is a project aimed at gathering information from open sources about social networks, phone numbers, domains, and IP addresses using Google Dorks. Plus, it can be installed on Linux as well as Termux with Windows. The tool has a very nice feature of maintaining a local database.

- **Holehe** is a powerful tool for detecting registered accounts by email. Holehe checks for email attachment to accounts on various platforms, including Twitter, Instagram, Imgur, and over 120 other sites. Our tool is very simple to install and use.

- **Ghunt** is a powerful and versatile OSINT tool designed for gathering information about users through their Gmail addresses. It provides access to the owner’s

name, identifiers, active Google services such as YouTube, Photos, Maps, and others. You can also get information about possible locations, Google documents, scheduled meetings in the calendar, and much more.

- **H8Mail** is a tool that scans the specified email inbox in its databases and provides a set of possible passwords. With its help, you can gain access not only to the email but also to all other accounts if the user reuses the same passwords. This is a very decent tool for checking against databases of various conditionally free services to search for leaked email passwords.

- **DarkGPT** offers advanced capabilities for working with leaked databases, significantly differing from previous tools based on ChatGPT, such as OSINVGPT, PentestGPT, and others. The Spanish pentester known as "luijait" recently introduced to the global community a novelty in the field of OSINT — the DarkGPT tool, which utilizes the power of GPT-4–200K for precise data leak analysis. Based on the latest advancements in artificial intelligence, it not only provides users with access to information but also tools for its analysis. DarkGPT stands out among its competitors due to the integration with GPT-4–200K, allowing for advanced data processing. The tool ensures secure access to leaked databases. Its interface, implemented through the command line, makes the tool accessible even for beginners in OSINT. The ease of use and intuitive interface significantly simplify the data collection and analysis process.

The Regulator doesn't care about the 'Truth': there is no perfect KYC

12 min read · Mar 25, 2024

Slava Solodkiy

- *Compliance is mistakenly perceived as a good/bad person proof*
- *Compliance isn't about 'to prevent 9\11', but when it happens, 'to quickly find who is involved'*
- *Real criminals use several layers of good people with good reasons for transactions*

"**Simply forget about KYC**; let anyone who desires a bank account have one, and use AI/ML to track the bad actors," said David Birch, and he was correct. Soups from Sardine.ai made a similar comment to me recently about working with high-risk clients — "KYC is just the simplest part, the real interest starts afterward."

Regulators aren't focused on the "truth" — what matters to them is that you've considered these types of risks. Compliance is often wrongly seen as a mechanism to differentiate good people from bad. In reality, **compliance is about "being trackable" (the ability to trace, to "follow the money")** through a set of dynamic parameters over time. It's vital to realize that no perfect KYC at the onboarding stage can safeguard you against fraud and scammers: only about 20% of malefactors can be caught upon registration.

Or how about something akin to **"ChatGPT for the financial sector"?** It's no longer challenging to develop a new AI. The crucial part is gathering high-quality big data to train this AI, which we have as we store unique data about transactions, onboarding, and EDD data. Especially, considering that starting from January 1st,

FinCEN is introducing a new regulation, AMLA, which requires banks to conduct KYCC, which affects correspondent and BaaS banks the most.

No individual is wholly bad or entirely good; broadly speaking, compliance isn't about "preventing September 11 from happening" but rather, when something does

happen, it's about "quickly identifying who is involved." There's no black and white in this — it's all about focusing on the customer, understanding them, the risks they bring, and how to monitor and manage those risks effectively.

Everyone has seen films where the FBI or other special services, exhausted from chasing a hacker, eventually propose they switch sides to assist in catching other hackers and criminals. So, why don't compliance departments hire individuals convicted (or currently imprisoned) for 'money laundering'? They understand compliance and can immediately spot suspicious patterns far better than any specialist. The same applies to risk and the creation of new credit products — instead of seeking advice from pampered business school graduates, who recommend stepping out of one's comfort zone while sipping 18-year-old whiskey in a vintage leather chair, why not consult those who have long been living outside their comfort zones?

High-Risk Compliance for BaaS and Correspondent Banks

Starting from January 1st, FinCEN introduced a new regulation, AMLA, which requires banks to conduct KYCC, which...

www.linkedin.com

As for banks (and licensed fintechs and digital banks): no regulator prohibits them from dealing with cryptocurrencies, cannabis dispensaries, foreigners, NGOs, PEPs, digital nomads and online influencers, Russians, and another 550 million people in 15 sanctioned countries, churches, contemporary art galleries, homeless individuals, and former prisoners... The regulator simply states: 1, if you wish to work with these groups, inform us; 2, and demonstrate that you're prepared for it.

"Follow the money" — remember, a 100% bad client never walks in and instantly does something terrible. In reality, it's initially decent individuals carrying out normal actions and transactions until an "anomaly" occurs. In 99.99% of cases, the anomaly is detected after the fact, necessitating a swift and efficient rewind. 'Truth' often hinges on the Hypothesis, which defines your risk tolerance.

I launched my previous startup, ArivalBank.com, five years ago. From the outset, the main challenge for Anastasia Cavallini , Justinas Kaminskas , Alexandre Pinot , and Sandra Ameziane... was compliance, followed by establishing better

correspondent banking relationships. This was a common issue faced by many in the fintech industry, including various BaaS platforms, digital banks, European EMIs, Asian e-wallet giants, IFEs, MTs/MSBs, and brokers. We secured our banking license in the US for ArivalBank.com in May 2021.

Then began the second phase: correspondent banking is not solely about payment rails; it also requires orchestrating compliance systems and understanding US regulatory requirements (as the primary route for correspondent banking services). We accomplished this ourselves, securing our US banking license and establishing daily operations with the Federal Reserve Bank of New York and FinCEN. We connected five banks in the correspondent banking chain, not just for payment rails, but also for orchestrating compliance in a "rely on" mode. By serving international clients from 26 countries, primarily from the US, UK, and EU, I've learned how to satisfy the requirements of bank partners and their regulators in key markets.

What could be done differently? You could integrate compliance to prevent transactions from becoming stuck, a significant issue for all correspondent banking providers. The main **bottleneck in correspondent banking and BaaS is compliance — there's a lack of trust and understanding between parties**, causing inquiries or concerns to halt the flow. In the worst-case scenario, when additional information is needed for a transaction or client, there's no seamless process for correspondent or BaaS banks, bank clients, and end-users to communicate and share information.

Compliance is often misunderstood as a binary determination of a person's character — good or bad. In reality, compliance focuses on creating a system capable of tracking financial activities ("following the money") through a set of evolving criteria over time. A crucial insight is that flawless Know Your Customer (KYC) processes at the initial stage of onboarding cannot entirely safeguard against fraud and scams; indeed, only 20% of fraudulent activities can be detected at this stage. The remaining 80% are identified during transaction monitoring. This necessitates the establishment of onboarding parameters that act **like a "net," designed to detect anomalous behavior patterns** during subsequent transactions, thereby enabling faster identification and the ability to "rewind" to trace connections.

Understanding the history (and purpose) of compliance is vital: its aggressive enforcement largely began post-September 11, 2001, as an effort to disrupt the

financial networks underpinning terrorist activities. The assumption is not that **compliance will prevent all illicit activities — human behavior is too complex for such a guarantee. Instead, when such activities occur, the goal is to swiftly identify and understand the parties involved.** Criminals often mask their transactions through layers of legitimate activities performed by unsuspecting individuals, making it nearly impossible to label someone as definitively bad at the point of onboarding. However, by setting up systems to notice anomalies or backtrack to identify accomplices, it is possible to significantly enhance the effectiveness of compliance efforts.

Regulators, for their part, do not expect infallibility in identifying the inherently "good" or "bad." In fact, a **record of no mistakes can be a red flag**, prompting further scrutiny and audits. When errors do occur, regulators are interested in:

- Who identified and reported the error — was it the institution, a client, a partner, or the regulator themselves?
- The promptness of the response — was the issue addressed immediately, or was there undue delay?
- Whether there was prior consideration of the risk type involved — even if the controls failed — or if the risk was entirely unforeseen.
- The planned corrective actions — generic responses might indicate a likelihood of recurrence, while specific, well-considered actions demonstrate a deeper understanding of the issue.

For institutions like ArivalBank.com, engaging with high-risk clients or operating within risky geographies and sectors requires a forthright acknowledgment of these increased risks and an assertion that managing them is not just a side task but a core specialization. Institutions must:

- Be transparent about their engagement with high-risk profiles, acknowledging it as a deliberate business choice.
- Conduct thorough risk analysis related to specific geographies and industries, detailing the unique challenges they present.
- Describe how they plan to mitigate and manage these risks through processes, technology, training, additional data sources, and an increased number of

screening questions.

Ultimately, if an institution can convincingly address these points, regulators will authorize them to proceed, monitoring for SARs (Suspicious Activity Reports) and, paradoxically, "mistakes." These errors, while not desirable, are part of the iterative process of refining compliance systems, risk profiles, and controls, thereby enhancing overall regulatory understanding and effectiveness.

In the context of Nansen.ID, our approach **is not to indiscriminately accept all applicants based on notions of charity or benevolence. Instead**, we advocate for banks and fintechs to embrace additional risks while demonstrating how to engage in more thorough vetting processes. Here's how we aim to exceed standard practices:

- **Utilizing Unconventional Databases:** We access a broader range of local and often unofficial databases not integrated with major compliance providers like Onfido, Veriff, ComplyAdvantage, SumSub, or Signicat. These include databases maintained by entities such as Navalny's Anti-Corruption Foundation, known for its anti-money laundering efforts; Khodorkovsky's Dossier; the Ukrainian "Peacemaker" database detailing war instigators and collaborators; and databases maintained by the international association of investigative journalists, including OCCR and Pulitzer Prize recipient Olesya Shmagun. Additionally, we leverage resources from the sanctions group at the Treasury and the US Senate, led by former US ambassador to Russia Michael McFaul. These sources offer rich data sets that are eagerly shared yet largely overlooked by compliance services focused on low-risk profiles.
- **Asking More Questions:** Beyond the standard inquiries, we delve deeper into an individual's employment and sources of income, aiming to gather detailed information to form a more complete understanding of their financial background.
- **Incorporating Affidavit Questions:** Recognized in jurisdictions with British legal traditions, affidavit questions add a legal layer to the vetting process. These aren't limited to queries about corruption and money laundering typically seen in visa applications; we also explore political stances, such as support for Putin/Lukashenko or views on the conflict with Ukraine. Lying in response to these questions is tantamount to perjury, highlighting the seriousness with

which they're treated. Some banks have already begun to include such probing questions in their processes, albeit quietly.

- **Leveraging Social Proof:** We encourage applicants to provide references from 3–5 individuals who can attest to their reliability, akin to the vetting process for employment or visa applications. This approach not only enriches the applicant's profile but also creates a network of accountability. In cases of fraud, this allows for a broader investigation into both the recommenders and those they've endorsed.
- **Requesting a List of Relatives** too: Given that politically exposed persons (PEPs) and others may launder money through family members rather than directly, compiling a list of relatives becomes an essential step in understanding and mitigating risk.

We don't just open our doors wider; we also refine our lens, enabling a deeper and more nuanced assessment of risk. This comprehensive approach doesn't seek the impossible task of discerning the "Truth" about an individual's nature. Instead, it ensures that we've thoroughly considered the types of risks presented and have made diligent efforts to document and verify them, thereby strengthening the integrity of our compliance processes and contributing to a safer financial ecosystem.

By adopting these measures, inspired in part by David Birch's initial proposition, "currently, banks and fintechs conduct customer due diligence (CDD) at entry and again at set annual intervals; this is costly (some banks spend over $500 million a year!), outdated, and often unpleasant for customers. A new paradigm — using automation and integrations for continuous or perpetual KYC (pKYC) — makes much more sense in today's world. Implementing pKYC requires solving problems in technology, data management, operations, and user experience, but promises to dramatically reduce fraud and operational costs. Companies that enable this —

which see pKYC as a way to solve compliance issues but also to strengthen customer value and LTV — stand to reap immense rewards." "Compared to consumers, B2B identification data is naturally more disparate. Business identification is indeed a vast topic, and we're just touching the tip of the iceberg in how enterprises unlock the context needed for more efficient money management. Many of the opportunities discussed in this letter — the shift to continuous pKYC, the potential for opening networks in credential issuance — are likely even greater in B2B than in B2C."

Ribbit Capital's new research: [digital] "banks may be best situated to become issuers of reusable...

Ribbit Capital has released a very good, detailed, practical, and detailed review of the digital identity market (for...

medium.com

In designing a robust architecture for compliance and data handling, the goal is to establish a system that initially allows for the collection of basic information (at a minimum, the name, email, and mobile number) and the **capability to incrementally gather more data without repetitively querying the user**. This approach positions you **as an AGENT** where users delegate their rights and consent for the Collection, Storage, Processing of data, and Transfer to third parties — but only at their explicit request. In the banking context, this translates to acting on the customer's behalf, managing account openings/closures, and transaction handling as if you were an extension of the bank itself.

Looking forward, the objective is to evolve into both a Data Processor and Data Controller while pursuing SOC1/SOC2 certifications. Regulators generally disapprove of indiscriminate data collection without a clear purpose. Thus, providing a well-defined rationale for data collection facilitates regulatory compliance — this is particularly relevant when partnering with banks, as it enhances clarity and transparency.

The ultimate aim is to simplify compliance-related processes, enabling users to **preemptively respond to inquiries, securely store their responses**, and readily provide necessary information as needed. However, the decision to approve or deny services rests with each individual provider, even though we may assist by providing

results from blacklist checks. This segregation of decision-making is a critical requirement in the U.S., with the EU still deliberating its stance.

With all that's been happening in Russia, Ukraine, and Belarus, the big question isn't just about how to keep onboarding clients who don't vibe with Putin and the war on Ukraine, especially those with Russian roots or passports. As Alex Nikityuk (from Revolut mafia) from YC-backed Maroo wrote here: due to recent events in Russia, Ukraine, and Belarus, the issue has arisen not so much of how to continue onboarding clients (who disagree with Putin and the war with Ukraine) with Russian passports or roots, but rather how companies like Deel, Revolut, and many others **should offboard such clients. And here, the question's cost is not theoretical — companies have already spent money attracting customers and their onboarding.** In this context, the EU is actively discussing the problem of opening (and closing) accounts for innocent customers (by the way, did you know that in sanctioned countries live more people than in the EU?). And it seems that what Nansen.ID is doing now is important not only in the context of Russia (Belarus and Ukraine), but also in 15 sanctioned countries where 550 million people live. Have you ever thought that not all people there support their regimes? And by "fanatically" disconnecting them from banking and other online services, we are not solving the problem, but only exacerbating it: locking the "disagreeing" inside their countries, leaving their assets to fuel the local economies, not allowing talented and active young entrepreneurs and scientists to leave these countries, weaken them by this, and strengthen the economies of the host countries?

In this context, the efforts of Nansen.ID are particularly relevant, extending beyond the immediate situations in Russia, Belarus, and Ukraine, to encompass 15 sanctioned countries home to 550 million individuals. It prompts a critical reflection: not everyone in these countries supports their government's actions. Cutting off access to banking and online services not only fails to address the underlying issues but exacerbates them. It isolates dissenters, retains their assets within these regimes, and prevents the emigration of innovative and active minds that could otherwise contribute to weakening oppressive governments and bolstering the economies of welcoming nations.

Nansen ID

NANSEN.ID is a digital identity solution designed for opposition members and political emigrants from sanctioned...

P.S. Here are two additional insights:

The notion that all Russians and Belarusians support Putin and Lukashenko is an oversimplification often held by compliance officers in banks from developed countries. This generalized perception can inadvertently push such clients towards banks involved in laundering "dirty money," unregulated cryptocurrencies, and crypto exchanges lacking proper compliance measures. It's vital to differentiate between rigid, "by-the-book" compliance and adaptable, self-learning compliance systems. For example, consider the scenario of accepting clients with past convictions, especially for economic crimes and money laundering. A traditional compliance officer might outright reject such prospects. However, a more nuanced approach reveals a broader opportunity.

In the U.S. alone, 80 million individuals with criminal records face barriers in opening bank accounts, renting apartments, and enrolling their children in schools, due to pervasive background checks. This statistic suggests that addressing and rehabilitating first-time offenders could significantly reduce overall crime rates. The "Scandinavian model," with its focus on support and rehabilitation, highlights the potential for integrating ex-offenders into society and the workforce, including the compliance sector of financial institutions.

Consider the innovative approach of '70 million jobs,' a Richard Bronson 's startup negotiating with corporations to hire ex-convicts, ensuring a double-check system for genuine rehabilitation and offering a second chance for these individuals. This model of collective responsibility and the potential for a digital bank specifically catering to ex-convicts illustrates the complexity of compliance and the need for a more inclusive, understanding approach.

Another point worth discussing is the concept of "consistency" and "inheritance" in the transition from onboarding to AML and transaction monitoring. This involves understanding and anticipating certain architectural nuances. For instance, categorizing contacts of bank customers as "Almost-Customers" and individuals who have transacted with bank customers but are not themselves customers as "Near-Customers" can refine AML monitoring strategies. Incorporating these segments into compliance processes, transaction monitoring, and marketing efforts

demonstrates the intricate balance between innovative customer engagement and rigorous compliance adherence.

Revolut's practice of analyzing customer contacts for potential outreach and compliance implications exemplifies the proactive approach required in modern banking. This methodology not only enhances customer experience and potential customer acquisition but also integrates compliance and operational efficiency seamlessly.

Such strategies underscore the importance of a sophisticated, forward-thinking approach to compliance, customer engagement, and the utilization of data for both security and growth. As the financial industry evolves, the intersection of compliance, technology, and social responsibility becomes increasingly crucial, necessitating innovative solutions that address the nuanced challenges of today's banking landscape.

Kyc Aml Baas Compliance Correspondent Bank

Edit profile

Written by Slava Solodkiy

954 followers · 244 following

chief believer x linkedin.com/in/vsolodkiy

Responses (1)

Slava Solodkiy

What are your thoughts?

They Are Much Better Than Your Chief Compliance Officer

Vladislav Solodkiy
Founder & ex-CEO @ ArivalBank.com, a.id, SREDA.VC | Early investor in 5 digital banks

March 26, 2024

The CIA has announced a new strategy for working with open-source information, aiming to expand and enhance the collection and analysis of data amidst the ever-growing information stream. The document, presented by the Office of the Director of National Intelligence (ODNI) and the CIA, discusses the development of methods for collecting, creating, and delivering intelligence from open sources (OSINT) until 2026. Special attention is given to the potential of artificial intelligence and machine learning in improving the processing of open data, as well as the risks associated with verifying the authenticity and reliability of information.

As part of the strategy, ODNI has enlisted leading cybersecurity expert Jason Barrett to implement key directions. His task is to integrate innovations into OSINT work based on the CIA's experience in this field over the last year. The CIA has also developed AI technology, similar to ChatGPT, for selecting relevant information from the vast amount of available data. This new tool automates the OSINT processing workflow, highlighting key data for analysis. Senator Mark Warner, the chair of the U.S. Senate Intelligence Committee, emphasized the importance of such tools, noting that the traditional view of prioritizing covert information collection is giving way to the recognition of the importance and effectiveness of using open data.

Open Source Intelligence (OSINT) involves searching and analyzing public information to ultimately gain new knowledge. Essentially, OSINT investigators primarily work with data that has already been published by someone at some point. States and corporations possess a vast amount of information, part of which can be found online or obtained upon request. However, the path to this data often lies through websites that are invisible to search engines, through cumbersome databases, little-known archives, and clunky interfaces. The investigator's skill lies in finding information, analyzing it, and making it understandable to a broad audience.

OSINT emerged in the 20th century as a military technology. One of the first entities specialized in such investigations was the Research and Analysis Branch of the American Office of Strategic Services, the precursor to the CIA. Today, open-source data intelligence methods are used by intelligence and government employees, as well as professional investigators and journalists.

OSINT primarily involves working with open data, but investigative teams sometimes use non-public sources. For instance, the investigations into the poisonings of Alexey Navalny or Sergei and Yulia Skripal are based on mobile operators' billing data (information about incoming and outgoing calls, SMS, internet traffic), passenger lists of trains and airplanes, leaked databases of commercial companies, and other data. Such information can be purchased on Telegram channels or in the darknet.

High-Risk Compliance for BaaS and Correspondent Banks

Starting from January 1st, FinCEN introduced a new regulation, AMLA, which requires banks to conduct KYCC, which affects correspondent and BaaS banks...

linkedin.com

Other open services used by OSINT investigators can be divided into groups:

- **Maps and satellite images**, not only the popular Google or Yandex but also Bing and OpenStreetMap (OSM). The latter operates on a Wikipedia-like principle — users can add and mark objects on the map themselves. For OSM, there's also the Overpass-turbo app, allowing for the download of coordinates for specific objects on the map, like all stores of a certain retail chain or all drinking water fountains in a city.
- **Services that allow searching by photo**, known not only to investigators but also to ordinary people. You upload a photo of a person, and the site shows you their social media page, and sometimes even friends they preferred to hide. Many of these platforms are paid but have limited free functionality, such as PimEyes or Search4Faces. There are also services providing information by phone number or car license plate.
- Commercial **company registries** reveal the company's founding date, authorized capital, legal address, and people associated with it.
- **Vehicle movement services.** The popular site Flightradar collects flight numbers, information about the starting and ending points of routes, registration number, country of registration, and other data about all flights. Similar services exist for tracking sea vessels.
- Services for **searching removed information.** Resources like WaybackMachine allow you to find and view old versions of websites — in case they have stopped working or their data has been removed.
- **Metadata analysis** systems can extract information from files of various formats about the date, time, and device that created a specific document. Or collect information about entire websites — when and by whom a domain was registered and which other domains are associated with that site. Services like who.is and Domain Tools allow for this.

EU lawmakers on easing the opening of bank accounts and...

The European Parliament adopted a resolution in connection with the murder of Alexey Navalny. It openly questions the legitimacy of Vladimir Putin as...

linkedin.com

For example, In "OSINT Techniques for Sensitive Documents That Have Escaped Into The Clear Web," Christina Lekati highlights a common vulnerability among organizations: sensitive documents inadvertently exposed online. Lekati notes that participants frequently discover documents posing significant risks to their organizations on the clear web, often due to employee errors or oversight. She emphasizes the importance of proactive searches to identify and manage these documents before they're exploited by threat actors. The article offers a tutorial on advanced search queries, using special characters and operators to refine searches for specific documents related to an organization. Lekati provides practical advice on how to use Google Dorking, a technique that utilizes special search strings to find sensitive information efficiently. Highlighting the potential goldmine of information that documents like contracts, internal processes, and admin credentials can represent, she warns of the exposure risk to competitors, the media, and other entities. To combat this, Lekati suggests several ready-to-use search queries involving operators that focus on finding specific file types, such as PDFs, PowerPoints, and Excel files. She encourages creativity in conducting OSINT checks and underscores the ease of mitigating such risks by eliminating or managing the exposure of sensitive documents. She advocates for OSINT as a defensive discipline, crucial for organizations to act proactively against potential security breaches.

Compliance Demystified: A Beginner's Guide

In today's fast-paced digital world, where every transaction leaves a digital footprint, the importance of compliance can't be overstated...

Medium

In 2015, 13-year-old Justin created a Twitter account under the nickname Intel Crab and invented a fake persona of a teenager from Donetsk. He collected videos, photographs, and quotes from people in the war-torn Donbas to post on his account. When Justin realized he had become popular—with thousands of followers—he stopped pretending to be a boy from Donetsk.

Justin decided to take a more serious approach. He began analyzing and verifying the information he gathered, as well as recreating context with additional tools like plane tracking services and satellite images. Now 20 years old, Justin regularly finds photos and videos from event locations, opens maps, and checks whether the specified geolocation matches what is visible in the images. He publishes his findings, for example, tracking changes in the amount of equipment at Russian military bases using satellite images, and monitored photos posted by Kadyrovites in Zaporizhzhia on VKontakte and Telegram, publishing their locations. Justin now has nearly 309,000 followers. This year, he is graduating from the University of Alabama and saving money to go to Ukraine to see the country not just on a monitor screen.

banned weapons and violations of humanitarian law in Syria since 2012 on the Brown Moses Blog. In 2014, he assembled a team and began investigating war crimes in Ukraine.

One of Bellingcat's most notable works is the investigation of the downing of Malaysia Airlines flight MH17 in Donetsk Oblast in July 2014. Journalists established that the missile that downed the plane was Russian and launched from territory controlled by Russian authorities. Using photos and videos by eyewitnesses who captured the Buk missile system in various locations, investigators tracked its movement from Russia to Ukraine. They reconstructed its route thanks to a cargo platform photographed in various places in Russia and Ukraine. Initially, the platform carrying the system had four Buk missiles, but the day after the plane's downing, only three were visible, and it was headed back towards Russia. Even the shadows cast by objects in photos and videos were important – using the SunCalc program, journalists calculated the approximate time of filming. Another significant detail was the smoke trail left by the missile. Using it, Bellingcat identified the missile's launch site on satellite images and eyewitness recordings.

The MH17 case brought popularity to both Bellingcat and the OSINT method itself. Media began to reference data from investigative teams more frequently, and some newsrooms established their own data and OSINT departments. The spread of the internet **allowed OSINT methods to extend beyond military intelligence and the professional community of investigators**, becoming a new form of digital activism.

Artificial intelligence could prevent errors and inaccuracies caused by the human factor. OSINT blogs constantly write that potentially AI could be delegated several tasks at once, such as determining the location of a shot or distinguishing between tanks and IFVs in satellite images. However, current software still struggles with this task. The military uses more advanced AI developments: their algorithms can recognize enemy troops in satellite images, predict the course of hypersonic missiles, and even autonomously attack enemy targets. (Read about how artificial intelligence learned to wage war.)

However, investigators can indeed have an impact on the world. The **results of work based on open data are sometimes considered by courts.** In 2018, the prosecutor of the International Criminal Court (ICC) issued an arrest warrant for Libyan General Mahmoud Werfalli, who carried out public executions. The ICC based its evidence on the analysis and geolocations done by the Bellingcat team. The Hague Court, which considered the case of the MH17 crash in Ukraine, also cited materials from Bellingcat investigations. The International Investigative Group on War Crimes in Ukraine, initiated by Eurojust, requested materials from a joint investigation by "Important Stories", OCCRP, and Der Spiegel on the supply of microelectronics and drones to Russia bypassing sanctions.

However, **investigators want their findings to be used more actively.** The Conflict Intelligence Team is currently working with other investigative projects to propose amendments to the legislation of EU and US countries. Investigators want their conclusions to have greater value in crime investigations. Only those who are inconvenienced by these investigations express outright distrust of OSINT researchers' materials.

The barrier to entry in OSINT is low—only internet access and free time are needed. No special education is required—there is no university or training program to graduate from and receive a diploma as an **OSINT investigator (although private courses are available**). Investigators themselves say that the main qualities needed for this work are patience

material, photos, and videos. It's very tedious and hard work," says Ruslan Leviev in an interview with Kit.

If you're already engaged in cyber investigations or want to gain knowledge in this field, I recommend applying for the GIJN's free online course (I've already applied). The GIJN course topics include: Basics of Digital Investigations, Threat Landscape: Malicious and Spyware, DNS: Websites and Infrastructure, Investigating Disinformation and Trolling, Network Analysis. Instructors: Craig Silverman , ProPublica reporter; Jane Lytvynenko , independent journalist (Guardian, BuzzFeed News, Joan Shorenstein Center at Harvard); Etienne "tek" Maynier, Amnesty Tech Lab staff; Luis Assardo , Reporters Without Borders staff and independent researcher. The course starts on April 29 and will run every Monday and Thursday for 6 weeks.

The Regulator doesn't care about the 'Truth': there is no perfect KYC

Compliance is mistakenly perceived as a good/bad person proof

Medium

We review and practice other popular OSINT tools:

- **Maigret** is an innovative tool designed for data analysis from various social platforms. It offers extensive capabilities for information gathering, user activity analysis, connection finding, and other functions. This tool has flexible settings for data collection and analysis, allowing you to choose social networks and save results into files. Maigret supports over 3000 sites for username searches. An excellent tool for username searches, it's maximally simple to install and equally easy to use.
- **Mr.Holmes** is a project aimed at gathering information from open sources about social networks, phone numbers, domains, and IP addresses using Google Dorks. Plus, it can be installed on Linux as well as Termux with Windows. The tool has a very nice feature of maintaining a local database.
- **Holehe** is a powerful tool for detecting registered accounts by email. Holehe checks for email attachment to accounts on various platforms, including Twitter, Instagram, Imgur, and over 120 other sites. Our tool is very simple to install and use.
- **Ghunt** is a powerful and versatile OSINT tool designed for gathering information about users through their Gmail addresses. It provides access to the owner's name, identifiers, active Google services such as YouTube, Photos, Maps, and others. You can also get information about possible locations, Google documents, scheduled meetings in the calendar, and much more.
- **H8Mail** is a tool that scans the specified email inbox in its databases and provides a set of possible passwords. With its help, you can gain access not only to the email but also to all other accounts if the user reuses the same passwords. This is a very decent tool for checking against databases of various conditionally free services to search for leaked email passwords.
- **DarkGPT** offers advanced capabilities for working with leaked databases, significantly differing from previous tools based on ChatGPT, such as OSINVGPT, PentestGPT, and others. The Spanish pentester known as "luijait" recently introduced to the global community a novelty in the field of OSINT - the DarkGPT tool, which utilizes the power of GPT-4-200K for precise data leak analysis.

analysis. DarkGPT stands out among its competitors due to the integration with GPT-4-200K, allowing for advanced data processing. The tool ensures secure access to leaked databases. Its interface, implemented through the command line, makes the tool accessible even for beginners in OSINT. The ease of use and intuitive interface significantly simplify the data collection and analysis process.

Navalny's Utopia for Realists

"The fight should not be solely against the fact that Russia is unfree, but that it is unhappy in all aspects. We have everything - yet we are an unhappy country.

linkedin.com

OSINT Skills Made Alexey Navalny and His Team Popular

It was the skills in Open Source Intelligence (OSINT) that helped Alexey Navalny and his team gain popularity. Most of their anti-corruption investigations are based on open data. One of their most striking investigations, "He Is Not Dimon to You," has garnered 46 million views. It details how friends, classmates, and trusted persons of Dmitry Medvedev own non-profit organizations that receive generous donations from oligarchs and state loans. The investigation triggered protests across Russia, and online shopping orders helped prove the connection between Medvedev and the man registered as the owner of his non-profit organizations. Shirts and sneakers ordered under the name and address of the formal owner eventually ended up with Medvedev, who appeared in them publicly without issue.

Their investigations have often put them at odds with powerful state actors, leading to legal challenges and personal risks. The work of Grozev, Shmagun, and Dobrokhotov exemplifies the critical role of investigative journalism in uncovering truth and holding the powerful to account. And regarding **compliance, KYC, and AML - I would recommend regulators, banks, and fintechs to learn from them** (as the CIA does), rather than from conferences and office research by major consulting firms.

Christo Grozev , Olesya Shmagun , and Roman Dobrokhotov are well-known investigative journalists and researchers renowned for their work in **exposing various illicit activities, money laundering** and government malfeasance, often involving high-profile cases and sensitive political matters.

Christo Grozev is known for his association with **Bellingcat**, an international collective of researchers, investigators, and citizen journalists that uses open-source and social media investigation. Grozev has been instrumental in investigations into the poisoning of Sergei Skripal and

Like Grozev, Olesya Shmagun has contributed to uncovering corrupt practices and AML. Her work, much like that of her peers, involves meticulous research and the use of open-source intelligence (OSINT) techniques.

Roman Dobrokhotov is the editor-in-chief of The Insider, known for his involvement in major investigative efforts alongside Bellingcat. Dobrokhotov has faced significant legal and political pressure within Russia, including police raids and being targeted by defamation lawsuits, as a result of his investigative work. His efforts have contributed to revealing the actions of Russian intelligence and military services in various international incidents.

Roman Dobrokhotov (read the full article on Wired) has become a notable figure in exposing the clandestine operations of Moscow's GRU military intelligence agency. Dobrokhotov's journey from a protester challenging Kremlin narratives to a fearless investigative journalist is marked by his crucial role in uncovering the identities and activities of Russia's most covert military spies and assassins, including their involvement in high-profile cases like the attempted assassination of Sergei Skripal with a nerve agent. Dobrokhotov's work not only exemplifies journalistic bravery but also underscores the vital importance of independent OSINT-media in challenging state-sponsored narratives and uncovering the truth via 'follow the money' approach.

Recently, Grozev, who won an Oscar for the documentary film about Navalny, has been focused (together with Dobrokhotov) on investigating the activities of Jan Marsalek from Wirecard and is preparing a documentary film about him. Following the unexpected death of Navalny, Christo has temporarily concentrated, along with other independent investigators, on collecting and analyzing data related to the death of the opposition figure, known for his investigations into corruption and money laundering, and those involved in it.

A most wanted man: Fugitive Wirecard COO Jan Marsalek...

Fugitive Wirecard COO Jan Marsalek wasn't just responsible for Germany's largest financial fraud in history. He was also a decade-long Russian spy.

The Insider

Hristo Grozev is a Bulgarian investigative journalist, media expert, and media investor, leading investigator at The Insider, previously worked with Bellingcat. He is one of the main authors of the investigation into the involvement of FSB Russia employees in the poisoning of Alexey Navalny. Winner of the European Press Prize and the Emmy Award for his investigative journalism. Around 2014, he started investigative journalism with Bellingcat: "I'm doing something I'm good at, finding things others miss, using my knowledge of Russia, the neighboring countries, including Ukraine, working with people in these countries, and being concerned about their governments (both in Russia and Ukraine) deceiving citizens. I do this voluntarily, spending my own funds on investigations."

In 2019, Grozev (together with Roman Dobrokhotov and Daniel Romein) was awarded the European Press Prize for Investigative Journalism & London Press Club Prize for Digital Journalism. In 2021, Bellingcat and CNN received an Emmy Award in the category of "Outstanding Investigative Report in News" for Hristo Grozev's investigation. They also made reports against NATO, which was illegally selling weapons to Saudi

during the migrant crisis. Grozev was accused of organizing the escape abroad of journalist Roman Dobrokhotov.

Grozev lived in Vienna for 20 years until 2023, where he was under police protection due to his exposes about Russia. In February 2023, he stated that he moved to the USA after Austrian authorities told him they could no longer guarantee his safety. In August 2020, Grozev stated in an interview with Deutsche Welle that the poisoning of Alexey Navalny was similar to the attempts on Emelyan Gebrev and Sergei Skripal, in which Russian special services are suspected.

Responding to a question about informants, Grozev said: "We work only with sources who understand the risk they are taking." He also denied any connection with the CIA, noting that Western intelligence had not even reached the information published by independent journalists. Grozev has bet on crowdsourcing: now anyone can join the work of investigative journalists, comparing data from flight tables with information about the time and place of high-profile poisonings and strange deaths. Several matches were immediately found.

From Dissident to Detective: On the Way to ShmagunGPT

OSINT Skills Made Alexey Navalny and His Team Popular

Medium

Olesya Shmagun (Princeton University , previously graduated from the Faculty of Journalism at Moscow State University in 2012, continued her studies in graduate school) - **Pulitzer Prize winner for the investigation of the Panama Papers**, co-founder of the publication "Important Stories", employee of the Center for the Study of Corruption and Organized Crime (OCCRP), four-time winner of the monthly journalism prize "Redkollegiya". In April 2017, as part of the International Consortium of Investigative Journalists along with 300 other journalists, received the Pulitzer Prize in the category for explanatory journalism for the investigation into the "Panama archive". In 2023, she graduated from the Woodrow Wilson School of Public and International Affairs at Princeton University, earning a master's degree in public policy.

Recently, Olesya and I were chatting about Nansen.ID and... ShmagunGPT, and I really think a tool for Enhanced Due Diligence (EDD), inspired by Olesya's investigative magic, is exactly what we need, especially in the worlds of banking and fintech. I threw an idea at Olesya about creating a digital identity solution for opposition figures or maybe even a digital bank for those in exile... With Olesya's incredible knack for digging into money laundering schemes, imagine digitizing her expertise to become a nemesis for money launderers everywhere with something like ShmaGUNGPT.

I dream of Nansen.ID (Metastate Ltd) as a business with a heart, channeling profits into the hands-on investigative work of journalists like Olesya, Christo, and Roman. Their investigative work provides insanely useful data for compliance in banks and fintechs—at the very least.

From a regulator's perspective, **KYC is less about knowing your customer and more about understanding where their money's from, how they got it, and where it's headed**. I've been around the block with bank compliance, and Olesya's battled against the baddies, uncovering corruption and laundering schemes. We're basically **enriching traditional**

Olesya's investigative methods. It'd be like an automated sidekick for other investigators and compliance officers.

Filling out the same personal info over and over for every new bank account, insurance policy, mobile plan, flight, hotel stay, apartment lease, and more—isn't it exhausting? That's where the last bit about "convenience" comes in (i.e., no need to re-answer if you've already addressed a question; digital ID will auto-fill the existing answer). That's for the end users.

For banks and other entities, it's crucial to grasp that the slickest KYC process at onboarding won't shield you from fraud and scammers: only 20% get caught at the get-go, while the other **80% are nabbed based on their transactions later on. To catch these guys later, you need to "cast a net" at onboarding** so that any anomalies in behavior can be spotted more swiftly, allowing a quick rewind to pinpoint accomplices. The **real slick criminals layer their operations with legit transactions by innocent folks—no system will red-flag them at onboarding**. But setting up the system to notice oddities sooner or swiftly backtrack to find connections? Totally doable.

Banks, fintechs, and insurers pay for this. But who really benefits? End users!, especially those who've been denied accounts or visas. It's a boon for the whole regulatory ecosystem, from visa centers and telecoms to hotels and airlines, even extending to online election services. In essence, it's a trade-off:

1, I get that my nationality (or additionally, my industry affiliation) blocks me from certain benefits and creates hurdles I'd rather not have; I want to enjoy those benefits.

2, I know you don't see me as the bad guy; you're just covering your bases because you can't tell us apart. So, my "payment" is becoming more open and transparent with you.

3, You accept this "payment," allowing you a closer look into my life, with the agreement that if someone linked to me steps out of line, they get cut off from the network of benefits.

It's a way of saying, "I'm cool, let me in," while also ensuring everyone plays by the rules. As in Ancient Greece: **exile from the polis** ("collective responsibility" in action) as the main possible "punishment".

Compliance crowdsourcing (and crowdfunding)

Investigations like the Panama Papers increasingly show that successful investigations against corruption and money laundering are carried out b...

nansen.id