



Money laundering techniques
24,458 subscribers

✓ Subscribed



Money Laundering Techniques - April 2025



Baptiste Forestier - CAMS [in](#)

Top Voice | spektr's Ambassador | Join a Vibrant Community of 40K+ Compliance Enthusiasts & Expand Your AML...



April 30, 2025

🔍 Once a month, explore the world of compliance with deep dives into old and new money laundering tactics, financial crime scandals, regulatory shifts, and groundbreaking innovations.

On April's menu we have:

- Job offer - Internal Control Lead (EMEA) at [Flowdesk](#) 🇷🇺
- The EBRD-Putin Fraud Evidence by [John Christmas](#) RU
- The Zhdanova Case: Cryptocurrency Laundering, Organized Crime, and the Global AML Challenge by [Valentina Topatigh](#) 🇷🇺🇸🇰
- FATF Recommendation: Targeted financial sanctions related to proliferation financing (7/40) 🇷🇺

Are you passionate about an AML related topic? 😊

Would you like to write about it and reach over 24k compliance professionals? 🔥

If so, just send me a message to work out the details! 😊

Also, if you could like and/or comment the post associated with this edition, that would be great to support the newsletter! 🙏

Job offer - Internal Control Lead (EMEA) at Flowdesk 🖥️

Do you want to be part of one of the most exciting players in digital asset market-making?

At Flowdesk, we're reshaping financial markets with cutting-edge tech, a global mindset, and a mission to bring transparency and liquidity to crypto. 🤝

As Internal Control Lead - EMEA, you'll be right where it matters:

- 🚀 Own and level-up our internal control framework across the region
- 🤝 Work hand-in-hand with top-tier teams across Compliance, Risk, and Ops
- 🚀 Act as a key advisor to leadership on control strategy, audit, and regulatory alignment

We're scaling fast, and this role is crucial to our next phase of growth.

You'll have the autonomy to make a real impact, plus the support of a highly collaborative and international team.

Based in Paris or London with hybrid flexibility and a top-tier compensation package. 📍

Ready to shape the future of digital finance with us?

Let's talk: <https://lnkd.in/gqj-EjPJ> 🚀

RU The EBRD-Putin Fraud Evidence

From: [John Christmas](#), whistleblower and co-author of 'KGB Banker'

On 26 February 2025, United Kingdom Prime Minister Keir Starmer announced a plan to increase defense spending from 2.3% to 2.5% of GDP. On 4 March 2025, European Commission President Ursula von der Leyen announced a 'ReArm Europe' plan to boost defense spending by 800 billion euros in part by waiving limits on budget deficits. This rush of spending, barely debated in the UK or EU, is motivated by fear of Russian President Vladimir Putin combined with fear that the United States now led by President Donald Trump might not defend Britain and Europe as previously assumed.

This is an enormous amount of money, especially considering the UK and EU are heavily overindebted already. Serious economic problems could

result. So why not try a different way to reduce Putin's threat? UK and EU policy makers should take a look at what their development bankers are doing because correcting their actions won't cost one cent and will instead save money. This is about combatting Russian money laundering in the UK and EU.

I used to be an employee of Parex Bank of Latvia. Parex was connected with Putin in several ways. Putin signed permission for Parex to open its branch in St Petersburg. The Spanish court in the prosecution of the Tambovskaya Mafia wrote that both named money launderers for this Putin-connected Mafia used platform accounts at Parex. And, Parex transferred over \$100 million to Eduard Khudainatov before giving liabilities to Latvian taxpayers. Khudainatov is identified by the FBI as a frontman for Putin. Additionally, other fraudulent 'loans' from Parex went to two oligarchs named in the 2018 US Treasury Putin Warning List.

I gave details of fraud at Parex to Latvian authorities in 2005, then fled the country. Parex collapsed exactly as I predicted, but then something amazing happened. Latvia discredited my whistleblowing by selling a Parex stake to the European Bank for Reconstruction and Development. The EBRD is funded by 76 countries including the UK and all of the EU member states. Later it was revealed that the sale was fake because Latvia secretly paid the EBRD to buy the stake to fool onlookers that Parex had not been looted.

The best source of evidence that the EBRD is a fraud is the European Commission's Eurostat. This is the official source of information for the EU and I continue to be astonished that Eurostat documents confirm the fraud however the fraud still continues. Possible explanations include mass fear and mass corruption. Also, a problem is low financial literacy since most people who learn that Latvia secretly paid the EBRD to cover up the looting of a European bank by Putin's oligarchs don't see why this is considered fraud.

The Eurostat 2014 letter evidencing the fraud between Parex, Latvia, and the EBRD is available on my website (<https://lawlesslatvia.com/wp-content/uploads/2014/10/Eurostat-letter-September-2014.pdf>) and also appeared on several Dutch media websites in 2014. In this letter, Eurostat clearly wrote that it allowed Latvia to keep Latvia's financial obligation from this deal 'confidential' which goes against the mission of Eurostat. This fake investment was already reversed.

The Eurostat 2018 report evidencing the fraud between Parex successor Citadele Bank, Latvia, and the EBRD used to be available on the Eurostat website (<https://ec.europa.eu/eurostat/documents/1015035/8054610/Final-findings-EDP-dialogue-visit-LV-7-9-June-2017.pdf>) and now is available on my website (<https://lawlesslatvia.com/wp-content/uploads/2018/12/Final-findings-EDP-dialogue-visit-LV-7-9-June-2017.pdf>). This report clearly states that Latvia has an obligation to reverse the EBRD investment in Citadele. This obligation, again, is being kept

secret by the Latvian government. This deal hasn't reversed yet and therefore losses keep increasing every year.

I've written articles for many websites and blogs explaining and showing this evidence. I've also done interviews for podcasts and presentations for conferences. The EBRD blocks all communication with me and never acknowledges knowing about the allegations and evidence. If the EBRD has a lawful explanation of what it is doing, why not say it? Two documentary films called 'Jumts' and 'Jumts 2' by [Nemelo.lv](https://www.youtube.com/watch?v=MSnGaOLBt_c) were repeatedly aired on RETV in Latvia (https://www.youtube.com/watch?v=MSnGaOLBt_c). These include the evidence, interviews with me, and interviews with others. However the fraud is still continuing, openly since it's all over the Internet and on television.

My most recent effort to expose the EBRD was screening my new documentary 'Bankers Game' at the UK Parliament on 28 January 2025. The event sponsor, MP Jim Shannon, got sanctioned by Russia on 23 April 2025. Russia didn't give a reason for the sanctioning so it's unknown whether this is connected. However it's difficult to imagine any other reason why Russia would have sanctioned Shannon. 'Bankers Game' is awaiting its premier at a film festival later this year and therefore is not available to the public yet. It includes interviews with several European politicians discussing the EBRD fraud and has original drone footage of arrested superyacht 'Scheherazade' which was purchased by Khudainatov on behalf of Putin.

The UK and EU should demand answers from the EBRD. The EBRD and Latvia should restate their financial statements back to 2009 to correct for the fake deals between the EBRD, Latvia, Parex, and Citadele. And, the EBRD should disclose a full list of similar deals in other countries where it announced bank investments but kept secret that it was paid to make those investments.

Some of the suspicious EBRD investments are in Ukio/Siauliu Bank of Lithuania, Ameriabank of Armenia, and Bank of Cyprus. All of those are connected with Putin's money laundering and they all have USD correspondent accounts thanks to the EBRD. Bank of Cyprus even forms a link between Putin's team and Trump's team. Plus, a person employed at the EBRD's Citadele controlled the shell company at the middle of the world-record-breaking 200-billion-euro money laundering through Danske Bank's branch in Estonia which was also connected with Putin.

I hope for a safe and peaceful future for the UK and EU. An easy first step to achieving this can be ending a major money-laundering channel. I think Putin will lose power if he loses access to his slush fund. Acknowledgement of the Eurostat evidence, and defunding and liquidating the EBRD which is the logical next step, is a good place to start. When liquidating, any recoverable amounts can be paid to victim countries like Latvia which lost billions of euros. This will cost nothing, save money for the UK and EU, and improve global security.

The Zhdanova Case: Cryptocurrency Laundering, Organized Crime, and the Global AML Challenge by [Valentina Topatigh](#)

Overview

As cryptocurrencies reshape the global financial system, criminals and state-linked actors are exploiting regulatory gaps. At the heart of a recent controversy stands Ekaterina Zhdanova—a Russian national suspected of orchestrating a sophisticated crypto laundering scheme that spans continents and involves different organized crime networks.

Who is Ekaterina Zhdanova?

Ekaterina Zhdanova is a Russian-born influencer, socialite, and businesswoman who once appeared on the cover of a prominent Russian fashion and culture magazine. Known for her luxurious lifestyle and ownership of several hotels and businesses in Moscow, Zhdanova carefully cultivated the image of a successful entrepreneur. However, behind the façade, she was allegedly running a multi-billion-pound illicit financial network spanning several continents.

Zhdanova is believed to have led Smart Group alongside Khzadi-Murat Magomedov and Nikita Krasnov. Far from being a conventional business, Smart Group allegedly operated as a global laundering front for transnational organized crime groups — most notably the Kinahan cartel, a powerful Irish crime gang. The group not only laundered money but also allegedly collaborated in illegal activities such as drug and firearms trafficking.

In addition to supporting criminal enterprises, Zhdanova and her network allegedly facilitated sanctions evasion for wealthy Russian clients, helping them illegally invest in the UK and move money out of Russia despite international financial restrictions. According to the UK's National Crime Agency (NCA), between late 2022 and summer 2023, Smart Group also funneled funds toward Russian suspected involvement espionage operations.

Another organization under investigation is TGR Group, reportedly linked to the same network and also tied into the Russian financial sector. Together, Smart and TGR routed laundered funds primarily through the Middle East and into over 30 countries worldwide. The investigations have been led by George Rossi and Elena Chirkinyan, uncovering significant connections between these organizations and sanctioned Russian interests.

In the years following the 2022 sanctions and during the Covid-19 pandemic, Smart and TGR expanded their operations. In the aftermath of

the sanctions, it became increasingly evident that elements of the Russian elite were turning to alternative financial networks to maintain access to Western economies — access that had been otherwise curtailed by financial restrictions. These groups provided crucial services that facilitated the circumvention of Know Your Customer (KYC) checks, enabling sanctioned individuals and entities to continue operating across international markets. Investigations later revealed that the TGR group, in particular, was actively supporting Russian-language media outlets such as Russia Today, which itself faced sanctions in jurisdictions including the United Kingdom. This relationship further highlighted the entanglement of financial and informational operations aimed at mitigating the impact of Western sanctions and sustaining pro-Russian narratives abroad.

How the scheme worked

The United Kingdom served as the central hub of the laundering operation, with Smart Group and TGR Group working in close coordination to conceal the origins and destinations of vast sums of criminal money.

The laundering process allegedly began with the collection of large volumes of physical cash from criminal enterprises. This cash was then converted into cryptocurrency, often through over-the-counter (OTC) brokers and unregulated exchanges, allowing for discreet transactions beyond the reach of traditional financial oversight. Once converted, the digital funds were transferred across borders, where they were exchanged for cash equivalents in other jurisdictions. Criminal groups would then use the cryptocurrency to reinvest in illicit operations, including the purchase of drugs and firearms, all without moving physical money — effectively erasing the traditional paper trail. Investigators observed that these exchanges occurred at scale, with street-level cash handovers followed almost immediately by crypto transfers of identical value, creating a seamless and difficult-to-trace financial loop. As a result, more than £20 million has been officially confirmed laundered, though the true amount is believed to be significantly higher.

Blockchain analysis further revealed that wallets linked to Smart and TGR had frequent interactions with Garantex, a Russian crypto exchange sanctioned by both the UK and the U.S. for facilitating payments to suppliers of components used in the Russia–Ukraine war. As law enforcement pressure intensified, the group reportedly raised its commission rates in late summer 2024 — a likely response to escalating risks and operational costs.

In 2023, the U.S. government sanctioned Ekaterina Zhdanova and her associates for their alleged involvement in a cryptocurrency-based laundering scheme designed to benefit sanctioned Russian oligarchs. The following year, in December 2024, the UK's National Crime Agency (NCA), as part of Operation Destabilise, uncovered an expansive financial network laundering illicit funds for organized crime groups across regions — from the UK to Latin America. The investigation also linked four businesses directly to the TGR Group. As of now, Zhdanova is in custody in France, awaiting extradition or further legal proceedings.

How crypto laundering works

At the heart of the Zhdanova network was a sophisticated process of laundering illicit funds through cryptocurrency — a method increasingly used by organized crime syndicates to move dirty money undetected across borders. This laundering cycle typically follows three stages: placement, layering, and integration.

Step 1: Placement

This is the initial phase, where criminal funds are introduced into the financial system. In Zhdanova's case, large amounts of cash collected by her network in the UK were used to purchase cryptocurrency, often through peer-to-peer (P2P) platforms, crypto ATMs, or unregulated exchanges. These entry points frequently bypass standard Know Your Customer (KYC) protocols, making them ideal for illicit activity. Shell companies were also reportedly used to buy crypto under the guise of legitimate business transactions, further masking the origin of the funds.

Step 2: Layering

Once the funds were converted into crypto, the next step was to obscure their trail. This was achieved through a variety of advanced obfuscation techniques:

- Mixers and tumblers were used to break up and redistribute coins in randomized amounts to new addresses.
- Chain-hopping — converting between different cryptocurrencies (e.g., Bitcoin → Monero → Ethereum) — added another layer of complexity to blockchain tracking. Privacy coins like Monero (XMR), Zcash (ZEC), and Dash, known for hiding transaction histories, were commonly employed.
- Cross-border transfers were facilitated using decentralized exchanges (DEXs) and P2P systems, allowing funds to leap between jurisdictions with little oversight.

Investigators observed real-time laundering activity in the UK, where street-level cash handovers were followed almost instantly by crypto transactions of the same value. This seamless exchange allowed criminal groups to operate globally without ever physically moving funds.

Step 3: Integration

The final stage of laundering involved reintroducing the "cleaned" funds into the legitimate economy. This was done by:

- Converting cryptocurrency back to fiat currency through exchanges — both regulated (using fake KYC documents) and unregulated.
- Purchasing NFTs and digital art to self-deal at inflated prices, a tactic that's notoriously difficult to trace.

- Investing in real estate, luxury goods, or services, effectively turning illicit crypto into assets that appear legitimate on paper.

Smart Group and TGR Group wallets were found to have repeated interactions with Garantex, a Russia-based exchange sanctioned by the UK and U.S. for facilitating payments to suppliers of components used in the Russia-Ukraine war — further implicating the network in geopolitically sensitive transactions.

Impact: How does her case highlight weaknesses in the global crypto AML framework?

The Zhdanova case is not an isolated anomaly but rather an example of systemic vulnerabilities in the global financial system — especially in the crypto space. As of 2025, crypto laundering poses significant challenges due to the rapid evolution of technology and regulatory gaps. Here are the key risks:

- **Rise of DeFi (Decentralized Finance):** DeFi platforms often lack KYC/AML protocols, making it easy for criminals to use flash loans, DEXs, or mixers to launder funds undetected.
- **Privacy Coins & Protocols:** Cryptocurrencies like Monero and Zcash are designed for anonymity, making them go-to tools for criminal organizations. After major hacks or laundering events, funds are often converted into these coins to erase their trail.
- **Regulatory gaps:** Criminals exploit jurisdictional loopholes, shifting operations to countries with lenient enforcement. Many unlicensed offshore exchanges still allow anonymous trading without identity checks.
- **Cross-Chain Bridges:** Bridges between blockchains (e.g., Ethereum ↔ Binance Smart Chain) allow funds to move with limited scrutiny, complicating forensic tracking.
- **Fake KYC / Identity Theft:** Fraudsters use stolen or synthetic identities to open verified accounts on platforms like Binance or Coinbase, then cash out crypto without arousing suspicion.
- **NFTs & Digital Goods:** NFTs offer a new avenue for self-laundering. Criminals mint and sell NFTs to themselves using different wallets funded with dirty crypto, masking the flow of funds as legitimate art sales.
- **Advanced Obfuscation Tools:** Tools like Wasabi Wallet, Samurai Wallet, and transaction “peeling” are designed to fragment and hide blockchain activity, defeating even advanced analytics firms like Chainalysis or Elliptic.
- **Lack of Global AML Standards:** Inconsistent enforcement of FATF Travel Rules and AML/CFT policies across countries creates blind spots where crypto criminals operate freely and with minimal risk.

Conclusion

Without urgent, coordinated global action, the innovations driving cryptocurrency will continue to outpace the safeguards meant to protect the financial system — and cases like Zhdanova’s will be only the beginning.

References

<https://www.dailymail.co.uk/news/article-14158197/The-glamorous-Russian-socialite-influencer-crypto-laundering-kingpin.html>

<https://www.sundayworld.com/crime/world-crime/glamorous-russian-socialite-ran-narco-money-laundering-ring-used-by-kinahan-gang/a838209978.html>

<https://www.bbc.com/news/articles/c70ezyrep1go>

<https://financialcrimeacademy.org/cryptocurrency-money-laundering-methods/>

FATF Recommendation: Targeted financial sanctions related to proliferation financing (7/40)

 The Financial Action Task Force (FATF) is an inter-governmental organization that sets international standards to combat money laundering, terrorist financing, and other threats to the integrity of the global financial system.

Its 40 recommendations provide a crucial framework for countries to adopt measures to combat these threats.

 Rec. 7 focuses on preventing the financing of the proliferation of weapons of mass destruction (WMDs).

While it shares similarities with Rec. 6, which addresses terrorism financing, Rec. 7 targets the unique challenges posed by proliferation financing.

Let's explore its specific aspects.

 Key elements of Rec. 7:

1 Implementation of UN Security Council Resolutions

Countries are required to enforce targeted financial sanctions as per United Nations Security Council Resolutions (UNSCRs) related to the prevention of WMD proliferation.

Key resolutions include UNSCR 1718 (2006) concerning North Korea  and UNSCR 2231 (2015) concerning Iran .

2 Understanding proliferation financing risks

Proliferation financing involves providing funds or financial services used to develop, acquire, or transfer WMDs, their delivery systems, and related materials.

It often involves sophisticated networks using front companies, shell corporations, and trade-based money laundering to disguise transactions.

Some items have both civilian and military applications (dual-use goods), making their detection challenging.

3 Legal and regulatory measures 🗑️

Authorities must have the power to freeze funds or assets of designated persons and entities without prior notice.

It's prohibited to make any funds or services available to designated individuals or entities, directly or indirectly. 🚫

4 Awareness and training 🎓

Financial institutions need to understand proliferation financing risks and implement appropriate controls.

It is important to provide sector-specific guidance to help detect and report suspicious activities related to proliferation financing.

Proliferation of WMDs poses a severe threat to international peace and security.

Thus, disrupting the financial networks that support these activities is crucial! 🌐

Are you passionate about an AML related topic? 😊

Would you like to write about it and reach over 23k compliance professionals? 🔥

If so, just send me a message to work out the details! 😊

Comments

👤👤👤 109 · 6 comments · 8 reposts



👍 Like

💬 Comment

➦ Share

Add a comment...



Most recent ▼



John Christmas • You
spy thriller novelist and whistleblower

1w ...

Hurray for Baptiste Forestier and his excellent publication 'Money Laundering Techniques' for including my latest piece with explanation and evidence of the EBRD-Putin fraud. You can't find this information in the institutional media like FT/Bloomberg/Reuters.

Like · 🌐 1 | Reply | 73 impressions



Robert L. Williams III, CAMS,CCI,CRFCC • 1st
AI Ethicist/Compliance Consultant @ Secure AI s Governance StartUp Sa..

1w ...

Excellent post/share Baptiste How are you?

Like · 1 | Reply



Valentina Topatigh • 2nd
labor compliance specialist @nike

1w ...

Thank you for sharing [Baptiste Forestier - CAMS!](#)

Like · 3 | Reply · 1 reply



Baptiste Forestier - CAMS Author
Top Voice | spektr's Ambassador | Join a Vibrant Community of 40...

1w ...

[Valentina Topatigh](#) It's my pleasure really, thank you for this great piece! 🙏

Like · 1 | Reply

Samuel Aidoo, Int.Dip(AML),MICA • 2nd
Head of Compliance & MLRO | AML, Financial Crime, Compliance Risk Pr...

1w ...

Great piece, well done

Like · 1 | Reply



Solandia Jurdi • 2nd
Compliance, AML/CFT & Virtual Assets Consultant | Founder & CEO @ Hi...

1w ...

Thank you for sharing!

Like · 1 | Reply



Money laundering techniques

Old and new money laundering methods, financial crime scandals, regulatory shifts, and much more explained every month.



Kenny, Frederic and 103 connections are subscribed

24,458 subscribers

✓ Subscribed

More articles for you





AML AWARENESS FOR NON-COMPLIANCE TEAMS:
WHY CROSS-FUNCTIONAL AWARENESS IS CRITICAL FOR PREVENTING MONEY LAUNDERING

By RT Compliance, Singapore
Compliance Expert

AML Awareness for Non-Compliance Teams: Why Cross-Functional Awareness is Critical for Preventing Money Laundering

The Compliance Corner



SHOROOQ

CRACKING DOWN ON ILLICIT FINANCE:
Compliance for a Bulletproof Institution

Maya Milan

Navigating AML & CFT Compliance

The Spotlight

 25 · 2 comments



MITIGATING AML RISK FOR VASPS
SOLUTIONS TO REDUCE THE RISK OF MONEY LAUNDERING

AML Risks and VASPs (Part 2) - Solutions to Mitigate the Risk of Money Laundering

Paul Byles

 4

