

The Top 10 AML & Sanctions Enforcement Cases.

Ten landmark failures. **The lessons every
compliance team needs.**

What happened, the effects on the business and market,
and the critical lessons learned from ten of the most
significant AML and sanctions enforcement cases
in history.

CONTENTS

Table of Contents

PART 1 · THE LANDSCAPE OF AML AND SANCTIONS ENFORCEMENT

1	Introduction: The High Cost of Non-Compliance	3
----------	---	---

PART 2 · THE TOP 10 CASE STUDIES

2	Case 1: BNP Paribas and the \$8.9 Billion Wake-Up Call (2014)	4
3	Case 2: Binance's Historic \$4.3 Billion Settlement (2023)	6
4	Case 3: 1MDB and Goldman Sachs' \$2.9 Billion Penalty (2020)	8
5	Case 4: Danske Bank's €200 Billion Baltic Scandal (2022)	10
6	Case 5: Commerzbank's \$1.45 Billion Dual Settlement (2015)	12
7	Case 6: Westpac's A\$1.3 Billion Fine for Systemic Failures (2020)	14
8	Case 7: Standard Chartered's \$1.1 Billion Double Offense (2019)	16
9	Case 8: ING Bank's \$619 Million Record-Setting Forfeiture (2012)	18
10	Case 9: British American Tobacco's \$635 Million North Korea Scheme (2023)	20
11	Case 10: Wachovia and the \$378 Billion Cartel Money Machine (2010)	22

PART 3 · ANALYSIS AND TAKEAWAYS

12	The Cases at a Glance: Quick-Reference Summary	24
13	Cross-Case Themes and Core Compliance Lessons	25

CONCLUSION

14	Why sanctions.io Is Your Ideal Screening Partner	27
15	Your Next Steps	28
	Sources	29

PART 1 · THE LANDSCAPE OF AML AND SANCTIONS ENFORCEMENT

Introduction: The High Cost of Non-Compliance

Money laundering and sanctions evasion are not victimless crimes. **They are the financial lifeblood of international terrorism, drug cartels, human trafficking rings, and rogue states.**

In response, global regulators have steadily intensified their scrutiny of the financial system, expanding their focus beyond traditional banking to encompass fintech, cryptocurrency exchanges, and multinational corporations.

When organizations fail to implement robust Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) controls, the consequences can be severe. Regulators no longer accept ignorance or technological limitations as excuses. The penalties for non-compliance now routinely reach into the billions of dollars, accompanied by deferred prosecution agreements, mandatory monitorships, executive resignations, and catastrophic reputational damage.

The Financial Action Task Force (FATF) estimates that money laundering accounts for between 2% and 5% of global GDP annually, representing trillions of dollars flowing through the legitimate financial system each year.¹ When institutions fail to act as the first line of defense, they become complicit in the harms that illicit finance enables, from funding weapons of mass destruction to financing child exploitation.

This e-book compiles ten of the most significant AML and sanctions enforcement cases in history. By examining what happened, the effects on the business and market, and the critical lessons learned, compliance professionals, legal teams, and senior executives can better understand the risks they face and how to build resilient compliance programs that prevent history from repeating itself.

2–5%OF GLOBAL GDP LAUNDERED
ANNUALLY (FATF)**\$20bn+**COMBINED PENALTIES
ACROSS THE TEN CASES**10**LANDMARK CASES, 2010 TO
2023

PART 2 · THE TOP 10 CASE STUDIES · CASE 1

BNP Paribas and the \$8.9 Billion Wake-Up Call

\$8.9bn

PENALTY

2014

YEAR SETTLED

Sanctions (Sudan, Iran, Cuba)

PRIMARY VIOLATION

Overview

In June 2014, BNP Paribas S.A. (BNPP), France's largest bank, agreed to plead guilty and pay a record-breaking \$8.9 billion to U.S. authorities for processing billions of dollars through the U.S. financial system on behalf of sanctioned entities in Sudan, Iran, and Cuba.² It was the first time a global bank had agreed to plead guilty to large-scale, systematic violations of U.S. economic sanctions.

What Happened

From 2004 through to 2012, BNPP deliberately moved over \$8.8 billion through the U.S. financial system on behalf of sanctioned entities. The bank went to elaborate lengths to conceal these transactions. Employees routed illegal payments through third-party financial institutions and systematically removed references to sanctioned entities from payment messages, a practice known as "wire stripping."

Remarkably, BNPP continued this conduct even after its own lawyers warned that the actions were illegal, prioritizing profit over compliance.² The majority of the illegal payments were made on behalf of Sudanese entities, including approximately \$4 billion for a financial institution owned by the Sudanese government, which was subject to U.S. embargo sanctions due to its role in supporting terrorism and committing human rights abuses.

Effects on Business and Market

The \$8.9 billion penalty was the largest ever imposed for sanctions violations at the time. BNPP was forced to terminate or separate 13 employees, including its Group Chief Operating Officer. The bank was temporarily suspended from clearing U.S. dollar transactions for certain business lines, severely impacting its global operations. The case sent shockwaves through the European banking sector, forcing institutions worldwide to fundamentally overhaul their sanctions screening processes and compliance governance structures.

LESSONS TO LEARN

The BNP Paribas case demonstrates that deliberate, systematic evasion of sanctions controls will be met with the full force of U.S. law, regardless of where a bank is headquartered. Stripping wire transfer information to bypass sanctions filters is a criminal act, and internal legal warnings must be heeded at the executive level. Crucially, any transaction clearing through the U.S. financial system is subject to U.S. sanctions laws, making the reach of OFAC truly global.

KEY FAILURE

Wire stripping and deliberate evasion, continued even after internal legal warnings.

PART 2 · THE TOP 10 CASE STUDIES · CASE 2

Binance's Historic \$4.3 Billion Settlement

\$4.3bn

PENALTY

2023

YEAR SETTLED

Sanctions + AML

PRIMARY VIOLATION

Overview

In November 2023, Binance, the world's largest cryptocurrency exchange, pleaded guilty to multiple criminal charges, including money laundering and sanctions violations, agreeing to pay \$4.3 billion in penalties to U.S. authorities.³ It was one of the largest corporate resolutions in the history of the U.S. Department of Justice, and the largest penalty in U.S. Treasury history.

What Happened

Between 2017 and 2022, Binance failed to report over 100,000 suspicious transactions linked to ransomware, darknet markets, and terrorist financing. The U.S. Treasury's Office of Foreign Assets Control (OFAC) found that Binance facilitated over 1.6 million apparent violations of multiple sanctions programs, processing transactions between U.S. users and users in sanctioned jurisdictions including Iran, Syria, Cuba, and North Korea.

Binance executives were found to have actively encouraged users to bypass the platform's weak compliance controls using VPNs, and management undermined its own compliance function in the pursuit of growth.³

Effects on Business and Market

Binance founder and CEO Changpeng Zhao was forced to resign and pleaded guilty to failing to maintain an effective AML program, personally paying a \$50 million fine. The company agreed to a five-year monitorship by the U.S. Treasury. The settlement marked a defining turning point for the cryptocurrency industry, signaling that digital asset platforms must adhere to the same stringent regulations as traditional financial institutions. OFAC noted that the maximum statutory penalty it could have levied was an extraordinary \$592 billion, underscoring the true scale of the violations.

LESSONS TO LEARN

The Binance case establishes that growth cannot be prioritized over compliance. Sacrificing AML and sanctions controls for market share will ultimately result in existential legal threats. Digital platforms must implement robust technological controls, including geo-fencing and IP blocking, to prevent access from sanctioned jurisdictions. The case also demonstrates the increasing trend of personal liability for executives, with regulators holding founders and CEOs directly accountable for systemic compliance failures.

KEY FAILURE

Compliance subordinated to growth, with users coached to bypass controls.

Operating in FinTech or digital assets? **The FinTech Compliance Playbook** covers screening controls built for high-growth platforms.

PART 2 · THE TOP 10 CASE STUDIES · CASE 3

1MDB and Goldman Sachs' \$2.9 Billion Penalty

\$2.9bn

PENALTY

2020

YEAR SETTLED

Corruption + money laundering

PRIMARY VIOLATION

Overview

The 1Malaysia Development Berhad (1MDB) scandal is one of the most audacious corruption and money laundering cases in history. In 2020, Goldman Sachs paid \$2.9 billion in global penalties for its role in facilitating the theft of billions from the Malaysian sovereign wealth fund.⁴

What Happened

Between 2009 and 2014, over \$4.5 billion was siphoned from 1MDB by corrupt officials and financiers, most notably the Malaysian financier Jho Low and associates of former Prime Minister Najib Razak. Goldman Sachs underwrote \$6.5 billion in bond offerings for 1MDB, generating approximately \$600 million in fees.

The bank's compliance and control functions failed to adequately investigate the suspicious nature of the deals, the involvement of third-party intermediaries, and the ultimate destination of the funds. The stolen money was used to purchase luxury real estate in New York and London, fine art, a superyacht, and even to co-finance the Hollywood film "The Wolf of Wall Street."⁴

Effects on Business and Market

Goldman Sachs suffered severe reputational damage and was forced to claw back compensation from current and former executives. The scandal upended Malaysian politics, leading to the conviction and imprisonment of former Prime Minister Najib Razak. Private banks that facilitated the illicit flows, including Switzerland's BSI and Falcon Bank, were shut down or lost their licenses in Singapore. The case prompted global regulators to significantly tighten oversight of sovereign wealth fund transactions and bond underwriting processes.

LESSONS TO LEARN

The 1MDB case makes clear that dealings involving Politically Exposed Persons (PEPs) and sovereign wealth funds require the highest levels of Enhanced Due Diligence (EDD). The presence of third-party facilitators who add no clear value to a transaction is a significant red flag that must trigger immediate investigation. Above all, a compliance program is only effective if the corporate culture genuinely empowers compliance officers to challenge and, if necessary, reject lucrative but high-risk deals.

KEY FAILURE

Failed PEP due diligence on a sovereign wealth fund and its intermediaries.

PART 2 · THE TOP 10 CASE STUDIES · CASE 4

Danske Bank's €200 Billion Baltic Scandal

\$2.0bn

PENALTY

2022

YEAR SETTLED

Money laundering

PRIMARY VIOLATION

Overview

Danske Bank, Denmark's largest lender, became the center of a massive European money laundering scandal when it was revealed that its Estonian branch processed approximately €200 billion in suspicious transactions between 2007 and 2015. In 2022, the bank pleaded guilty in the U.S. and agreed to pay \$2 billion in penalties.⁵

What Happened

Danske's Estonian branch aggressively courted non-resident clients, primarily from Russia and other former Soviet states. These clients used shell companies registered in the UK, Cyprus, and offshore havens to funnel funds of unclear origin into the European banking system.

Internal whistleblowers raised alarms as early as 2013, but executive management in Copenhagen repeatedly ignored the warnings. The Estonian branch was not fully integrated into the bank's central AML monitoring systems, creating a critical blind spot that persisted for nearly a decade.⁵

Effects on Business and Market

The bank's CEO resigned, and its stock price dropped by nearly 50% following the public revelation of the scandal. Danske faced criminal investigations across several jurisdictions and lawsuits from investors. The scandal forced European regulators to drastically tighten AML oversight and accelerated the development of stricter EU directives regarding beneficial ownership transparency and cross-border AML supervision.

LESSONS TO LEARN

Non-resident portfolios, particularly those involving clients from high-risk jurisdictions, carry extreme risk and require exhaustive KYC and continuous monitoring. The Danske Bank case is a powerful reminder that ignoring internal reports of suspicious activity turns manageable problems into catastrophic institutional failures. Multinational banks must ensure that all foreign branches are fully integrated into global AML monitoring and governance frameworks, with no exceptions.

KEY FAILURE

Ignored whistleblowers and a foreign branch left outside central AML monitoring.

PART 2 · THE TOP 10 CASE STUDIES · CASE 5

Commerzbank's \$1.45 Billion Dual Settlement

\$1.45bn

PENALTY

2015

YEAR SETTLED

Sanctions + Bank Secrecy Act

PRIMARY VIOLATION

Overview

In March 2015, Germany's Commerzbank AG agreed to pay \$1.45 billion to U.S. authorities to settle violations of both U.S. sanctions laws and the Bank Secrecy Act (BSA), making it a rare case where a single institution was penalized simultaneously for both sanctions evasion and fundamental AML failures.⁶

What Happened

From 2002 to 2008, Commerzbank processed \$263 million through the U.S. financial system on behalf of Iranian and Sudanese entities.⁶ Employees in Frankfurt deliberately altered payment messages to hide the involvement of sanctioned parties from the bank's own U.S. branch, in some cases explicitly instructing colleagues never to mention the Iranian connection.

Separately, the bank's New York branch failed to maintain an effective AML program, allowing over \$1 billion related to the Olympus accounting fraud to flow through its accounts undetected.

Effects on Business and Market

The settlement required Commerzbank to terminate responsible employees and install an independent compliance monitor. The dual nature of the fines, punishing both deliberate sanctions evasion and fundamental AML failures, highlighted the deep interconnectedness of financial crime risks. The case reinforced the U.S. government's commitment to prosecuting foreign banks that abuse their access to the U.S. dollar clearing system.

LESSONS TO LEARN

The Commerzbank case illustrates that hiding information from your own compliance departments or foreign branches constitutes willful criminal intent and will be treated accordingly by regulators. Weaknesses in transaction monitoring consistently expose institutions to both money laundering and sanctions risks simultaneously. Furthermore, creating bespoke "safe payment solutions" to help high-risk clients avoid detection is a direct and serious violation of compliance duties.

KEY FAILURE

Internal deception of its own U.S. branch, alongside basic AML failures.

PART 2 · THE TOP 10 CASE STUDIES · CASE 6

Westpac's A\$1.3 Billion Fine for Systemic Failures

A\$1.3bn

PENALTY

2020

YEAR SETTLED

AML / CTF

PRIMARY VIOLATION

Overview

In 2020, Australian bank Westpac agreed to pay a record A\$1.3 billion penalty to the financial intelligence agency AUSTRAC for massive, systemic breaches of anti-money laundering and counter-terrorism financing laws. It remains the largest civil penalty in Australian corporate history.⁷

What Happened

Westpac failed to report over 23 million international fund transfers to AUSTRAC between 2013 and 2019, totaling over A\$11 billion.⁷ The bank's IT systems were poorly configured, meaning transaction data was simply not captured or transmitted to regulators.

Most alarmingly, the bank failed to conduct appropriate due diligence on transactions to the Philippines and Southeast Asia that matched known typologies for child exploitation material. AUSTRAC flagged payments showing patterns consistent with child exploitation, but Westpac's systems were incapable of identifying or escalating these transactions.

Effects on Business and Market

The sheer scale of the failure, combined with the horrific nature of the underlying crimes that the bank's systems had facilitated, led to intense public outrage. Westpac's CEO Brian Hartzer and Chairman Lindsay Maxsted were both forced to resign. The case triggered a massive overhaul of compliance technology across the entire Australian banking sector and prompted a national conversation about the adequacy of AML controls at major financial institutions.

LESSONS TO LEARN

The Westpac case establishes a clear principle: IT failures are compliance failures. If your systems cannot accurately capture and report transaction data, your AML program is fundamentally broken, regardless of how robust your written policies may be. Banks must actively monitor for specific transaction patterns associated with high-harm crimes, and the processing of millions of transactions requires automated, scalable monitoring solutions. Manual sampling is wholly insufficient.

KEY FAILURE

IT failures: 23 million transfers never reported to the regulator.

How automation closes this gap: **The Future of Compliance Automation.**

PART 2 · THE TOP 10 CASE STUDIES · CASE 7

Standard Chartered's \$1.1 Billion Double Offense

\$1.1bn

PENALTY

2019

YEAR SETTLED

Sanctions (Iran)

PRIMARY VIOLATION

Overview

Standard Chartered Bank (SCB) faced two major enforcement actions regarding U.S. sanctions violations.⁸ After a 2012 settlement, the bank was penalized again in April 2019, agreeing to pay \$1.1 billion to U.S. and UK authorities for further violations of sanctions against Iran. The repeat offense made it one of the most high-profile examples of a financial institution failing to remediate compliance deficiencies after regulatory intervention.

What Happened

The 2019 action concerned conduct that had not been disclosed during the 2012 settlement: SCB's Dubai branch had continued to process transactions for Iranian entities until 2011. Employees in the Dubai branch actively helped clients set up front companies in the UAE to obscure their Iranian connections, processing approximately 9,500 transactions worth \$240 million through the U.S. financial system on behalf of these hidden Iranian clients.

The bank's compliance program was insufficiently robust to detect employee-assisted evasion.

Effects on Business and Market

The repeat offenses severely damaged SCB's credibility with global regulators. The bank was forced to extend its deferred prosecution agreement for an additional two years and pay massive new fines across multiple jurisdictions, including the UK's Financial Conduct Authority. The case highlighted the intense regulatory focus on the Middle East as a transshipment point for sanctioned goods and funds, and the particular risks posed by UAE-registered front companies.

LESSONS TO LEARN

Repeat offenses following a regulatory action will result in exponentially higher penalties and a permanent loss of regulatory goodwill. Relying on superficial corporate registry documents in high-risk jurisdictions is insufficient; the ultimate beneficial ownership of all counterparties must be verified. Compliance programs must also have specific mechanisms to detect when relationship managers are actively colluding with clients to evade controls.

KEY FAILURE

Repeat offense, with staff helping clients build front companies.

PART 2 · THE TOP 10 CASE STUDIES · CASE 8

ING Bank's \$619 Million Record-Setting Forfeiture

\$619m

PENALTY

2012

YEAR SETTLED

Sanctions (Cuba, Iran)

PRIMARY VIOLATION

Overview

In June 2012, Dutch financial institution ING Bank N.V. agreed to forfeit \$619 million for illegally moving billions of dollars through the U.S. financial system on behalf of sanctioned Cuban and Iranian entities.⁹ At the time, it was the largest fine ever levied against a bank for sanctions violations, setting the benchmark for the wave of major enforcement actions that would follow.

What Happened

From the early 1990s until 2007, ING Bank processed over 20,000 transactions worth more than \$2 billion in violation of U.S. sanctions.⁹ ING's wholesale banking division in Curaçao systematically removed references to Cuba in payment messages.

The bank also provided U.S. dollar trade finance services to sanctioned entities through misleading messages and shell companies, and even fabricated bank endorsement stamps to fraudulently process U.S. dollar travelers' checks. Critically, senior corporate managers and legal and compliance departments were aware of and approved this conduct.

Effects on Business and Market

The ING case set the precedent for the massive enforcement actions that would follow against other European banks for similar “wire stripping” practices. It forced global banks to recognize that OFAC would aggressively police the use of the U.S. dollar as a reserve currency, and that the long arm of U.S. sanctions law extended to any institution that touched the U.S. financial system, regardless of its domicile.

LESSONS TO LEARN

The ING case demonstrates that historical practices, even those stretching back decades, are not safe from regulatory scrutiny. The fact that conduct “has always been done this way” provides no legal protection. Trade finance operations require specialized compliance checks to ensure that underlying goods and counterparties are not sanctioned. Altering any payment data to bypass screening filters constitutes a deliberate criminal act that will attract the full force of U.S. enforcement.

KEY FAILURE

Wire stripping, approved by management, legal and compliance.

PART 2 · THE TOP 10 CASE STUDIES · CASE 9

British American Tobacco's \$635 Million North Korea Scheme

\$635m

PENALTY

2023

YEAR SETTLED

Sanctions (North Korea)

PRIMARY VIOLATION

Overview

In April 2023, British American Tobacco (BAT) and its subsidiary BAT Marketing Singapore (BATMS) agreed to pay over \$635 million to U.S. authorities for orchestrating an elaborate, decade-long scheme to sell tobacco products to North Korea in violation of U.S. sanctions.¹⁰ The case demonstrated that sanctions enforcement extends far beyond the financial sector.

What Happened

In 2007, BAT publicly announced it was exiting the North Korean market. In reality, it spun off its North Korean sales to a third-party company in Singapore while maintaining total control over all relevant aspects of the business.

Between 2007 and 2017, this scheme generated approximately \$415 million in U.S. dollar transactions. North Korean purchasers used front companies to pay the Singaporean entity, which then funneled the money back to BATMS and BAT, deceiving U.S. banks that processed the payments into believing there was no North Korean connection.¹⁰

Effects on Business and Market

The penalty was the largest ever imposed by the DOJ for North Korean sanctions violations. The case demonstrated that sanctions enforcement is not limited to financial institutions; multinational corporations in the manufacturing and export sectors face identical risks. It also highlighted how the illicit tobacco trade is a major funding source for North Korea's nuclear weapons program, with counterfeit cigarettes estimated to be one of the most lucrative items in North Korea's illicit portfolio.

LESSONS TO LEARN

Corporate shell games designed to maintain business in sanctioned countries while publicly claiming to have exited constitute a severe and deliberate compliance violation. Manufacturing and export companies must maintain robust sanctions screening programs covering their entire supply chain and distribution networks, not just their direct customers. Companies must verify the ultimate destination of their products, not just the identity of the immediate buyer in a transit hub.

KEY FAILURE

A corporate shell game in the non-financial sector.

Screening suppliers, distributors and partners: **The Third-Party Risk Screening Guide.**

PART 2 · THE TOP 10 CASE STUDIES · CASE 10

Wachovia and the \$378 Billion Cartel Money Machine

\$160m

PENALTY

2010

YEAR SETTLED

AML (drug cartels)

PRIMARY VIOLATION

Overview

In 2010, Wachovia Bank (now part of Wells Fargo) settled a federal investigation by paying \$160 million in fines and forfeitures for failing to monitor an astonishing \$378.4 billion in transactions linked to Mexican drug cartels. The case remains one of the most striking examples of the scale at which legitimate banking infrastructure can be weaponized by organized crime.¹¹

What Happened

Between 2004 and 2007, Wachovia processed hundreds of billions of dollars from Mexican casas de cambio (currency exchange houses) without adequate AML controls.¹¹ The bank ignored blatant red flags, including bulk cash shipments, sequentially numbered travelers' checks with suspicious signatures, and deposits vastly exceeding normal business needs.

A London-based AML officer, Martin Woods, repeatedly filed Suspicious Activity Reports (SARs) regarding these transactions, but Wachovia management not only ignored the warnings but actively marginalized the whistleblower. The laundered funds were ultimately used by the Sinaloa cartel to purchase airplanes for drug smuggling.

Effects on Business and Market

The case exposed the terrifying scale at which legitimate banking infrastructure was being utilized by violent drug cartels. While the \$160 million fine was widely criticized as a “slap on the wrist” compared to the \$378 billion transaction volume, the reputational damage was immense. The investigation unfolded as Wachovia collapsed during the 2008 financial crisis and was acquired by Wells Fargo. The case also became a landmark example of the human cost of compliance failures, as the laundered funds directly financed the brutal violence of the Mexican drug war.

LESSONS TO LEARN

Correspondent banking relationships with foreign financial institutions, such as currency exchanges, require rigorous oversight of the underlying customer base, not just the immediate counterparty. Retaliating against compliance officers who identify suspicious activity destroys institutional integrity and guarantees regulatory intervention. Most profoundly, this case is a reminder that compliance failures are not merely regulatory or financial events; they directly facilitate real-world violence and human suffering.

KEY FAILURE

Ignored SARs and retaliation against the whistleblower.

PART 3 · ANALYSIS AND TAKEAWAYS

The Cases at a Glance: Quick-Reference Summary

The following table provides a high-level overview of all ten cases for quick reference.

#	INSTITUTION	YEAR	PENALTY	PRIMARY VIOLATION	KEY FAILURE
1	BNP Paribas	2014	\$8.9 billion	Sanctions (Sudan, Iran, Cuba)	Wire stripping; deliberate evasion
2	Binance	2023	\$4.3 billion	Sanctions + AML	Ignored compliance for growth
3	Goldman Sachs / 1MDB	2020	\$2.9 billion	Corruption + money laundering	Failed PEP due diligence
4	Danske Bank	2022	\$2.0 billion	Money laundering	Ignored whistleblowers; no branch integration
5	Commerzbank	2015	\$1.45 billion	Sanctions + BSA	Internal deception; AML failures
6	Westpac	2020	A\$1.3 billion	AML / CTF	IT failures; 23M unreported transactions
7	Standard Chartered	2019	\$1.1 billion	Sanctions (Iran)	Repeat offense; employee-assisted evasion
8	ING Bank	2012	\$619 million	Sanctions (Cuba, Iran)	Wire stripping; management-approved
9	British American Tobacco	2023	\$635 million	Sanctions (North Korea)	Corporate shell game; non-financial sector
10	Wachovia	2010	\$160 million	AML (drug cartels)	Ignored SARs; whistleblower retaliation

PART 3 · ANALYSIS AND TAKEAWAYS

Cross-Case Themes and Core Compliance Lessons

While these ten cases span different industries, decades, and jurisdictions, the root causes of their compliance failures are strikingly consistent. By analyzing these massive enforcement actions together, compliance teams can identify the critical vulnerabilities that lead to disaster.

Tone at the Top Is Everything

In almost every case, from BNP Paribas to Binance, senior executives were either aware of the compliance gaps or actively encouraged the circumvention of controls. A compliance program is only as effective as the culture that surrounds it. When leadership prioritizes short-term profit over legal obligations, compliance officers are disempowered and the institution is exposed to catastrophic risk.

Technology Must Match the Threat

Westpac's failure to report millions of transactions and Commerzbank's manipulation of payment filters both demonstrate that outdated or misconfigured technology is a massive liability. Modern AML and sanctions compliance requires real-time, automated screening and monitoring systems capable of processing high transaction volumes and detecting complex patterns. Institutions that rely on manual processes or legacy systems are operating in a state of permanent vulnerability.

The Danger of High-Risk Segments

Whether it was Danske Bank's non-resident portfolio, Wachovia's correspondent banking clients, or 1MDB's PEP involvement, institutions consistently fail when they aggressively pursue high-risk business without implementing correspondingly rigorous Enhanced Due Diligence (EDD). The higher the risk of a customer or transaction, the more intensive the oversight must be.

Transparency and Early Remediation

Covering up errors, as seen in Standard Chartered's repeat offenses or BAT's decade-long corporate shell game, always results in harsher penalties. Regulators consistently reward proactive self-disclosure and swift, demonstrable remediation. The cost of early transparency is almost always far lower than the cost of a cover-up.

The Regulatory Response Has Been Transformative

These cases collectively reshaped global AML and sanctions regulation.¹² The EU's AMLD5 and AMLD6 directives introduced stricter beneficial ownership registries and whistleblower protections. The U.S. AML Act of 2020 expanded FinCEN's powers and introduced federal beneficial ownership reporting, which was narrowed in 2025 to apply primarily to foreign companies registered to do business in the U.S. FATF has updated its recommendations to address virtual assets and new payment methods. The regulatory landscape that exists today is, in large part, a direct product of the failures documented in these ten cases.

WHAT COMES NEXT

The EU's new Anti-Money Laundering Authority (AMLA), established under Regulation (EU) 2024/1620, began operating in 2025 and is due to start direct supervision of the highest-risk financial institutions in 2028, the most centralized enforcement mechanism in European AML history.

TURN THE LESSONS INTO A WORKFLOW

Most of these failures trace back to fragmented controls. **The Unified Guide to Screening** shows how to bring sanctions, PEP and adverse media screening into a single process, and the **Sanctions Screening Guide** walks through setting one up from scratch.

CONCLUSION · CHAPTER 14

Why sanctions.io Is Your Ideal Screening Partner

The cases outlined in this e-book demonstrate that manual checks and outdated systems are no longer sufficient to protect your business. Regulators demand real-time, comprehensive screening against global sanctions lists, PEP databases, and criminal watchlists, and they expect institutions to prove that their controls are actively working, not merely that policies exist on paper.

sanctions.io provides an enterprise-grade, AI-powered screening solution designed to meet the rigorous demands of modern compliance. Our platform is trusted by over 400 customers, including financial institutions, fintech companies, crypto exchanges, and multinational corporations across the globe.

Comprehensive coverage	Access continuously updated global sanctions lists, PEP data, adverse media, and criminal watchlists from a single, unified API.
Seamless integration	Our RESTful API integrates smoothly into your existing onboarding and transaction monitoring workflows, with no disruption to your operations. We also offer native integrations for HubSpot, Salesforce, and Shopify.
High reliability	Benefit from a 99.995% uptime guarantee, ensuring your screening processes never bottleneck your business.
Advanced matching algorithms	Reduce false positives while ensuring you never miss a critical match, utilizing fuzzy logic, phonetic matching, and AI-powered name resolution.
Continuous monitoring	Move beyond one-time checks at onboarding. Monitor your entire customer base in real time and receive instant alerts when a customer's risk profile changes.

Comparing providers? The **Vendor Selection Guide** sets out the features that matter most, and pricing is transparent on the **sanctions.io pricing page**.

— CONCLUSION · CHAPTER 15

Your Next Steps

- 1 Assess Your Current Exposure.** Review how your organization currently screens customers, counterparties, and payment flows against sanctions lists and PEP databases. Identify where you rely on one-time checks, where monitoring gaps exist, and where false positives are creating friction for your compliance team.
 - 2 Map the Failures to Your Own Program.** Use the ten case studies in this guide as a diagnostic framework. Ask whether your institution shares any of the structural weaknesses identified, including siloed compliance functions, inadequate transaction monitoring, insufficient due diligence on high-risk clients, or a culture that subordinates compliance to revenue.
 - 3 Understand Your Risk Profile.** Not sure where to start? Use the free **Global Risk Screening Calculator** to get a clear picture of your screening risks and requirements in under three minutes.
 - 4 Book a Call.** If you are ready to strengthen your AML and sanctions compliance program, **schedule a call** with the sanctions.io team to discuss your workflow, risk exposure, and implementation priorities.
-

With sanctions.io, you can build a compliance program that is faster, more consistent, and better aligned to today's sanctions and financial crime risk environment.

Book a call

Prefer to talk it through? See how your compliance process can go from inefficient to simple, scalable and unified.

REFERENCES

Sources

- 1 **Financial Action Task Force (FATF), "Money Laundering"**
fatf-gafi.org
- 2 **U.S. Department of Justice, "BNP Paribas Agrees to Plead Guilty and to Pay \$8.9 Billion," June 30, 2014**
justice.gov/news
- 3 **U.S. Department of Justice / OFAC, "Binance Holdings Limited Agrees to Plead Guilty," November 21, 2023**
justice.gov/news
- 4 **U.S. Department of Justice, "Goldman Sachs Charged in Foreign Bribery Case," October 22, 2020**
justice.gov/news
- 5 **U.S. Department of Justice, "Danske Bank Pleads Guilty to Fraud," December 13, 2022**
justice.gov/news
- 6 **U.S. Department of Justice, "Commerzbank AG Admits to Sanctions and Bank Secrecy Violations," March 12, 2015**
justice.gov/news
- 7 **AUSTRAC, "AUSTRAC and Westpac Agree to Proposed \$1.3bn Penalty," September 24, 2020**
austrac.gov.au/news-and-media
- 8 **U.S. Department of Justice, "Standard Chartered Bank Admits to Illegally Processing Transactions," April 9, 2019**
justice.gov/news
- 9 **U.S. Department of Justice, "ING Bank N.V. Agrees to Forfeit \$619 Million," June 12, 2012**
justice.gov/news
- 10 **U.S. Department of Justice, "British American Tobacco to Pay \$629 Million," April 25, 2023**
justice.gov/news
- 11 **U.S. Department of Justice, "Wachovia Bank Enters into Deferred Prosecution Agreement," March 17, 2010**
justice.gov/news
- 12 **U.S. Department of the Treasury, OFAC Civil Penalties and Enforcement Information**
ofac.treasury.gov/civil-penalties-and-enforcement-information
- 13 **sanctions.io Blog, "Top 5 Money Laundering Cases"**
sanctions.io/blog
- 14 **sanctions.io Blog, "Top 5 Fraud Cases from Around the World"**
sanctions.io/blog