Addressing the Hidden Dangers of Bad Data in Your Fraud & AML System

Sources: FinCEN FY2023 Year in Review; LexisNexis Risk Solutions (2024) True Cost of Financial Crime Compliance; NYDFS Part 504; Federal Reserve SR 11-7.

Data quality is a regulatory, financial, operational risk and what it means to you.

See through your data®

Gracie Ortiz, COO

Navigation System

Imagine you're driving in an unfamiliar city and fully relying on your GPS. Now, let's say the GPS has **bad data**—old maps, mislabeled roads, missing street names.

At first, you don't notice. The voice confidently tells you: "*Turn left in 200 feet.*"

You turn... but instead of a main road, it's a dead end. You reverse, try again, and waste 10 minutes.

Later, it routes you through a construction zone. You lose another 15 minutes in traffic.

Finally, it mislabels a highway exit, sending you 10 miles the wrong way. By the time you reach your destination, you're late, stressed, and questioning whether you should trust GPS at all.

The Risk: Why “Bad Data” = Real $$$ Dollars & Orders

NASA’s $327 Million Mars Orbiter Loss (1999)

NASA lost the **Mars Climate Orbiter** because one engineering team (NASA) used imperial units (pounds of force), while another (Lockheed Martin) used metric units (newtons).

The mismatch wasn’t caught, so the spacecraft entered Mars’ atmosphere at the wrong angle and disintegrated.

A single data translation error destroyed a $327 million mission and years of research.

Lesson: Bad data isn’t just “inconvenient”, it can literally burn up in thin air.

The Risk: Why “Bad Data” = Real $$$ Dollars & Orders

The London Cholera Epidemic (1854)

During a cholera outbreak in London, bad assumptions about data almost cost more lives. At the time, authorities believed cholera spread through **“bad air”** (miasma).

Dr. John Snow challenged this with data mapping, plotting cholera deaths and finding they clustered around a single water pump on Broad Street.

Once the pump handle was removed, the epidemic subsided.

Lesson: Acting on wrong data/assumptions (“bad air”) almost blinded people to the true cause. Correcting data saved lives.

The Risk: Why “Bad Data” = Real $$$ Dollars & Orders

Hawaii False Missile Alert (2018)

On January 13, 2018, Hawaiians got a terrifying emergency alert: “BALLISTIC MISSILE THREAT INBOUND TO HAWAII. THIS IS NOT A DRILL.”
It was caused by a **bad data entry during a system test,** an operator clicked the wrong option on a dropdown menu.
Panic spread for 38 minutes until officials clarified it was a false alarm.

Lesson: Bad interface and data entry mistakes can create mass panic at scale.

The Risk: Why “Bad Data” = Real $$$ Dollars & Orders

Google Flu Trends Failure (2008–2015)

- Google tried to predict flu outbreaks using search data.
- Initially impressive, but it began to **overestimate flu cases by 140%**.
- Why? People’s search behavior didn’t always match actual illness data.

Lesson: Big data without validation against reality can be dangerously misleading.

The Risk: False Positives & Data Gaps

False positives swamp teams, delay investigations, and hide real risk;

industry estimates often cite up to ~95% false-positive alert rates in legacy rules systems.

Data mapping gaps, truncation, or stale reference data → missed sanctions hits, poor segmentation, and under-reported SARs.

Regulators tie it together: governance + data lineage + validation across AML models and sanctions filters are mandatory—not optional

Executive Summary

Bad data quietly undermines fraud & AML controls—driving false positives, missed risks, and regulatory exposure.

Scale is massive: ~4.6M SARs and 20.8M CTRs filed in FY2023; compliance cost across US + Canada ≈ $61B/year.

Regulators are explicit: validate the integrity, accuracy, and completeness of monitoring & filtering data (NYDFS Part 504); model outputs depend on input data quality (SR 11-7).

Recent US enforcement actions (TD Bank, Capital One, USAA, U.S. Bank, Citi) show data/monitoring failures trigger nine-figure+ outcomes.

A 90-day diagnostic + targeted remediation can reduce alert noise 20–40% while improving true-positive capture and exam readiness.

How Big Is the Problem?

FY2023 filings: ~4.6 million SARs (~12.6k/day) and ~20.8 million CTRs (~57k/day).

294,000+ institutions & e-filers submit BSA data; 2.3M+ FinCEN Query searches by authorized users.

Compliance cost (US & Canada): ≈ $61B annually; 99% of FIs saw rising costs (2024).

What “Bad Data” Looks Like – Typical Failure Modes

Metric / Finding	What it shows	Source(s)
33.5% of SARs had at least one error in critical fields	In an audit of ~1.75 million SARs (discrete + batch) filed between May 2013 and April 2014, the U.S. Treasury’s Office of Inspector General found that one or more data quality errors existed in 33.5% of the filings. Office of Inspector General	OIG report, “The Universal Suspicious Activity Report and Electronic Filing Have Helped Data Quality but Challenges Remain”

What “Bad Data” Looks Like – Typical Failure Modes

SARs Complexity

- FinCEN Files = narratives + spreadsheets with 100s of transactions
- Highly detailed in some cases; incomplete in others

Data Gaps & Errors

- 20%+ missing addresses (even for bank’s own clients)
- 50%+ wrong country codes (e.g., China tagged as “CH”)
- Blank fields across critical data points

Systemic Issues

- 2018 Treasury IG audit: 33.5% SARs had errors
- No correction mechanism in place

Response

- Treasury: reforms 'balance quality with urgency & usefulness'

Data Extraction Challenge

- 85 journalists across 30 countries
- 17,600+ additional records processed

Technical Solution

- ICIJ built Datashare platform to extract, clean, and share records

What “Bad Data” Looks Like – FinCEN Data Challenges

Despite the high stakes, many institutions struggle to achieve good SAR data quality. Here are some key challenges:

- **Legacy systems & data silos.** Information about transactions, customer profiles, branch identifiers, or KYC data may be dispersed across systems and not well integrated.
- **Human error** in filing and narrative writing: staff may be rushed, undertrained, or not fully aware of what “good narrative” means.
- **Tradeoff pressure:** Many institutions judge compliance by volume of SARs filed, rather than by quality. That can push teams toward superficial reports.
- **Changing regulatory expectations.** Regulators’ demands evolve, so what was acceptable before may not be sufficient now.
- **Ambiguity in “suspicious” criteria.** Some activity is borderline; detecting it requires judgment and context. That can lead to inconsistencies across filers.
- **Validation limitations.** While electronic filing and form validation help, not every missing or wrong field can be caught by automated checks.
- **Volume overload.** With millions of transactions and SARs, scale makes human review harder. Mistakes slip through.
- **Feedback loops are weak.** Often, financial institutions receive little or no feedback from law enforcement on which filed SARs were useful or why some were rejected or ignored. That makes it harder to improve future reporting.

What “Bad Data” Looks Like Typical Failure Modes

Incomplete/incorrect KYC: missing beneficial ownership, stale occupation/NAICS, poor geodata → wrong risk rating.

Monitoring inputs: unmapped payment fields, truncated free text, inconsistent counterparty IDs; poor time zone/currency handling.

Sanctions/watchlist screening: name-matching not tuned; un-screened ISO 20022 fields; outdated lists or transliteration logic.

Case management: broken lineage between alert → investigation → SAR/NO SAR; poor outcome labels for model feedback.

Governance: ad-hoc threshold changes with no back testing; vendor models without validation; undocumented data transformations.

87 hits

first_name	last_name
Daddy	Duran
daddy	kenan
Daddy	Zeke
daddy	ira
daddy	ej
Daddy	B.
Daddy	D
Daddy	Agovino
Daddy	& Mommy
Daddy	Horvath
daddy	horvath
daddy	frazier
Daddy	Account
Daddy	Account
Daddy	Horvath

23 hits

first_name	last_name
Fuck	Off
Fuck	Off
Fuck	Off
Fuck	Off
Fuck	You
Fuck Me In The Car	John
Fuck	Boi
Fuck	Off
Fuck	Off
Fuck	Off
Fuck	Off
Fuck	You
Fuck	Off
Fuck	Off
Fuck	You

56 hits

first_name	last_name
mommy	boy
Mommy	Banker/LoanOfficer
Mommy	Spencer
Mommy	Banker/LoanOfficer
Mommy	Moore
Mommy	Moore
Mommy	Banker/LoanOfficer
Mommy	Moore
Mommy	Moore
Mommy	Ravdin
Mommy	Sones
Mommy	Lovely
Mommy	Lovely

3 hits

first_name	last_name
Goofy	Mouse
Goofy	Ellis
Goofy	Mouse

first_name	last_name
Minnie	Mouse
minnie	mouse

84 hits

first_name	last_name
Jane	Doe
Jane	Doe
Jane	Doe
Jane	Doe
Jane	Doe
Jane	Doe
Jane	Doe
Jane	Doe
Jane	Doe
Jane	Doe
jane	doe
Jane	Doe
Jane	Doe
Jane	Doe
Jane	Doe

US Banks need to Focus On: Data & Monitoring Lessons

- TD Bank (Oct 10, 2024): DOJ guilty plea + multi-agency actions (≈$3B). Findings included multi-year monitoring gaps and employee misconduct; monitor imposed and growth limits (OCC).
- Capital One (Jan 15, 2021): $390M FinCEN penalty for willful/negligent BSA violations tied to high-risk check casher activity and failures in program effectiveness.
- USAA FSB (Mar 17, 2022): $140M FinCEN penalty for willful BSA violations; thousands of SARs late/incorrect; program weaknesses known since 2017.

US Banks need to Focus On: Data & Monitoring Lessons

- U.S. Bank (Feb 15, 2018): $185M FinCEN penalty (+OCC $75M) for capping alerts/investigations to manage workload → willful BSA violations.

- Citigroup/Citibank (Oct 2020 & Jul 2024): $400M OCC penalty and Cease & Desist for risk/data governance; later $136M for failing to meet remediation milestones.

U.S. Bank Penalized for Violations of Anti-Money Laundering Laws

Banks are required to conduct risk-based monitoring to sift through transactions and to alert staff to potentially suspicious activity. Instead of addressing apparent risks**, U.S. Bank capped the number of alerts its automated transaction monitoring system would generate to identify only a predetermined number of transactions for further investigation, without regard for the legitimate alerts that would be lost due to the cap.**

"U.S. Bank is being penalized for willfully violating the Bank Secrecy Act, and failing to address and report suspicious activity. **U.S. Bank chose to manipulate their software to cap the number of suspicious activity alerts rather than to increase capacity to comply with anti-money laundering laws**," said FinCEN Director Kenneth A. Blanco. "U.S. Bank's own anti-money laundering staff warned against the risk of this alerts-capping strategy, but these warnings were ignored by management. U.S. Bank failed in its duty to protect our financial system against money laundering and provide law enforcement with valuable information."

U.S. Bank systemically and continually devoted an inadequate amount of resources to its AML program. Internal testing by U.S. Bank showed that alert capping caused it to fail to investigate and report thousands of suspicious transactions. Instead of removing the alert caps, the bank terminated the testing. U.S. Bank also allowed, and failed to monitor, non-customers conducting millions of dollars of risky currency transfers at its branches through a large money transmitter. In addition, U.S. Bank filed over 5,000 Currency Transaction Reports (CTRs) with incomplete or inaccurate information, impeding law enforcement's ability to identify and track potentially unlawful behavior.

US Banks need to Focus On: Data & Monitoring Lessons

Citibank

ARTICLE II COMPTROLLER'S FINDINGS Section (4):

"The OCC has identified the following deficiencies, noncompliance with 12 C.F.R. Part 30, Appendix D, or unsafe or unsound practices ***with respect to the Bank's data quality and data governance, including risk data aggregation and management and regulatory reporting****:..."*

ISO 20022 Payments Data: Risk & Opportunity

Richer, structured data (parties, remittance info) can improve sanctions screening & AML if ingested and mapped correctly.

Coexistence/translation with legacy MT can cause data truncation or field loss; creating blind spots if not detected and remediated.

Industry guidance now emphasizes data quality for screening across ISO 20022 fields and clear practices to detect truncation and exchange missing data.

Where Hidden Data Risk Creeps In Typical Pipeline

- **Ingestion:** un-mapped sources; schema drift; failed loads silently defaulting values.
- **Normalization & enrichment:** wrong entity resolution; stale sanctions lists/PEPs; outdated geocoding; weak transliteration support.
- **Monitoring & screening:** incomplete field coverage; poor calibration; lack of back testing and outcome analysis.
- **Case management & reporting:** broken lineage; inconsistent SAR narratives; weak QC and peer review.
- **Governance & model risk:** absent data SLAs; missing challenger models; inadequate documentation and change control.

Where Hidden Data Risk Creeps In Typical Pipeline

- **Completeness** ≥ 99.9% on key KYC & payment fields; zero “silent nulls.”
- **Accuracy** validated quarterly via sampling/independent checks; ≥ 99.5% for sanctions-relevant fields.
- **Timeliness SLAs:** sanctions lists ≤ 4h; KYC refresh per risk tier; alert disposition within policy.
- **Lineage & traceability:** end-to-end field mapping; reproducible transformations; automated data drift alarms.
- **Outcome-linked:** every alert has final label → feedback loop for tuning/ML with robust Model Risk Management (MRM) controls.

Regulatory Expectations - What Examiners Will Ask

- Show evidence you identify all data sources and validate integrity/accuracy/quality; prove complete & accurate transfer into monitoring systems.
- Document detection scenarios/thresholds and how they map to your risk assessment; show pre-/post-implementation testing results.
- Demonstrate model risk controls (development, validation, ongoing monitoring, outcomes analysis) and effective challenge.

Regulatory Expectations - What Examiners Will Ask

- OFAC: risk-based sanctions program, internal controls, testing/audit, and training; governance & timely list updates.

- NYDFS Part 504: annual Board/Senior Officer certification with supporting evidence; treat it like SOX for AML data.

90-Day Diagnostic – Quick Wins + Evidence for Exams

- **Weeks 0–2:** Map critical data elements (CDEs) across KYC, payments, alerts, SARs; stand up drift & completeness monitors; freeze current thresholds.
- **Weeks 2–6:** Parallel run data quality fixes; re-map ISO 20022 fields; back test screening coverage; implement reviewer checklists & SAR QC.
- **Weeks 6–10:** Tune thresholds/segmentations using outcome labels; pilot ML triage where allowed; harden lineage & audit trails.
- **Weeks 10–12:** Update policies/procedures; prep examiner-ready artifacts; finalize KPI baseline & target glide path.

Remediation Blueprint (6–12 Months)

- **Data:** central CDE catalog + lineage; automated quality rules; ISO 20022 full-field ingest; sanctions list ops with <4h SLA.
- **Models/Rules:** outcomes-driven tuning; challenger models; sanctions fuzzy-match optimization per name-type/language.
- **Process:** case taxonomy standardization; SAR narrative templates; QC sampling; analyst assist with explainable features.
- **Governance:** Model Risk Management (MRM) policy aligned to SR 11-7; change control; independent validation; model inventory with risk tiering.
- **People/Org:** scaled L2/L3 triage; training on typologies & ISO 20022 data; clear RACI from alert → SAR/NO SAR.

KPI Dashboard (Track Risk & Efficiency)

- **Alert quality:** FP rate ↓, precision/recall ↑; true-positive yield per 1k alerts.
- **Timeliness:** median time-to-first-touch; % alerts/SARs within policy SLA.
- **Data health:** % completeness by CDE; drift alarms; sanctions list freshness; translation/truncation incidents.
- **Governance:** % models validated on schedule; open MRM issues aging; change tickets with back tests attached.
- **Outcomes:** SAR hit-rate uplift; law-enforcement feedback; exam findings resolved on time.

Deep Dive: TD Bank (2024–2025)

- Outcome: DOJ guilty plea (BSA conspiracy) + civil actions (FinCEN $1.3B; OCC $450M + growth cap; Fed $123.5M).
- Findings: monitoring gaps (2018–2024), missed/ignored red flags; employee misconduct; independent monitor required.
- Relevance: demonstrates how monitoring coverage gaps and control failures escalate to multi-agency, multi-year remediation.

Deep Dives: Capital One & USAA

- Capital One (2021): $390M FinCEN penalty for willful & negligent BSA violations tied to high-risk business (check cashers); program failures and reporting gaps.

- USAA FSB (2022): $140M FinCEN penalty; willful BSA violations; thousands of SARs inaccurate/late; acknowledged program weaknesses by 2017.

Deep Dives: U.S. Bank & Citigroup/Citibank

- U.S. Bank (2018): $185M FinCEN penalty (+OCC $75M) for capping monitoring alerts/investigations and understaffing → willful BSA violations.

- Citigroup/Citibank (2020 → 2024): $400M OCC penalty and C&D for data governance/internal controls; additional $136M in 2024 for remediation delays.

ISO 20022 Action Checklist for AML/Fraud

- **Map & ingest all relevant ISO fields**; document one-to-one/one-to-many mappings from Swift MT → ISO 20022 MX and vice versa. (where appropriate and applicable)
- **Implement truncation detection** & RFI workflows; monitor for field-loss incidents during coexistence.
- **Re-tune sanctions screening** for richer name/address structures; ensure transliteration and script coverage.
- **Update typology libraries & ML features** to leverage remittance and party data; add back testing.

Next Steps
Tailored to Your Bank

- Select 2–3 business lines (ie: retail, MSB, Prepaid, credit, loans, etc) + 2 payment rails for a 90-day diagnostic; prioritize high SAR volume and high sanctions exposure.
- Stand up executive-visible KPI dashboard; lock in target reductions for false positives & time-to-first-touch.
- Book independent model/data validation (aligned to SR 11-7) to pre-answer examiner questions.
- Document annual Part 504 certification evidence package (if NY-regulated).

Appendix: Key Sources (Links)

- FinCEN Year in Review FY2023 (pdf) - https://www.fincen.gov/system/files/shared/FinCEN_Infographic_Public_508FINAL_2024_June_7.pdf
- LexisNexis Risk Solutions (2024) True Cost of Financial Crime Compliance: https://risk.lexisnexis.com/about-us/press-room/press-release/20240221-true-cost-of-compliance-us-ca
- NICE Actimize false positives brochure: https://www.niceactimize.com/Lists/Brochures/aml-reducing-false-positives-in-transaction-monitoring-brochure.pdf
- SR 11-7 Model Risk Management (pdf): https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf
- NYDFS Part 504 (pdf): https://business.cch.com/BFLD/NYDFS-Part504-07012016.pdf
- OFAC Framework (pdf): https://ofac.treasury.gov/media/16331/download?inline=
- TD Bank actions: DOJ case page; FinCEN; OCC; Federal Reserve; Reuters coverage

Appendix: Key Sources (Links)

- Capital One (2021) FinCEN: https://www.fincen.gov/news/news-releases/fincen-announces-390000000-enforcement-action-against-capital-one-national
- USAA FSB (2022) FinCEN: https://www.fincen.gov/news/news-releases/fincen-announces-140-million-civil-money-penalty-against-usaa-federal-savings
- U.S. Bank (2018) FinCEN & OCC: https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-national-association-violations-anti-money-laundering; https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-17.html
- Citi (2020 OCC order): https://www.occ.gov/static/enforcement-actions/ea2020-056.pdf ; (2024 fine): https://www.reuters.com/business/finance/us-bank-regulators-fine-citi-136-million-failing-address-longstanding-data-2024-07-10/