ANNUAL COMPLIANCE REVIEW

2021

The reset year: post-pandemic risk, new statute, new priorities

By Dominic Suszek

Founder and CEO, Global RADAR Solutions

Table of Contents

A Note from the Founder

When I sat down to write this review, I kept coming back to the same thought: 2021 was the year compliance stopped being treated like a back-office function and started being treated like a strategic risk. The Anti-Money Laundering Act of 2020 had just become law on January 1, the largest expansion of the Bank Secrecy Act since the Patriot Act. The Corporate Transparency Act was sitting on top of it, creating a federal beneficial ownership registry that the United States had refused to build for two decades. FinCEN published the first government-wide AML and CFT priorities in June, telling the industry for the first time exactly what to focus on. And the pandemic, far from slowing things down, had thrown years of digital-only onboarding, remote work, stimulus fraud, and synthetic identity attacks at compliance teams that were still using 2019 playbooks.

What I wanted this review to do was simple. Give a Chief Compliance Officer something they can read in twenty minutes and walk away with a clear picture of what changed, what it meant for their program, and how to think about it in the context of the year that came before. We launched these annual reviews because our customers kept asking for a single source of truth that did not require subscribing to four newsletters and reading two hundred law-firm alerts. This is that document for 2021.

A short note on how this review is organized. We start with the five developments that mattered most. Then we work through the other items that did not make the top of the headlines but materially affected how programs were built and tested. Then we look at the year in enforcement, with a table of the notable fines, the regulators that brought the actions, and the amounts. We close with a forward-looking note that sets up the year that followed. Where I think there is a lesson to be learned, I say so plainly. Where I think the industry is overreacting, I say that too.

Trends and Year-over-Year Comparison

Compared to 2020, the headline shift was scope. 2020 was a year of crisis response: pandemic fraud, PPP screening, and emergency SAR filing. 2021 was a year of statutory rebuild. The AML Act and the CTA together represented the largest expansion of the BSA framework since the Patriot Act in 2001. Where 2020 forced compliance teams to react fast, 2021 forced them to rebuild slow. That tension defined the year. Programs that had been built for a steady-state, branch-based banking model now had to absorb new whistleblower protections, raised civil penalties, mandated risk-based supervision, a national priorities framework, and the prospect of a federal beneficial ownership registry, all while continuing to fight pandemic-era fraud at record volumes.

The enforcement signal also changed. 2020 enforcement totals had been muted in part because regulators were managing pandemic disruption. 2021 saw the return of program-level enforcement at scale, headlined by the NatWest criminal AML case in the UK and the Capital One BSA action in the US. Most institutions absorbed the 2021 statutory changes without an immediate budget increase, then realized over the second half of the year that the new perimeter would require multi-year investment. The trend line moving into 2022 was clear: more entities pulled into the perimeter, more data collection at account opening, more pressure on transaction monitoring quality, and a regulator population that was about to be measured by how well the new statute was implemented in practice.

There is also a quieter trend worth naming. Boards started asking compliance leaders questions they had not asked in years. How are we tuned for the eight national priorities? What is our exposure to convertible virtual currency? Where are we on the BOI rule even though the deadline is years out? The questions were not always sophisticated, but the fact that they were being asked at the board level was itself a shift. Compliance had moved from a tactical function reporting up to legal or risk, to a strategic function reporting up to the board agenda.

The Five Most Important Items of 2021

This is the short list. If a Chief Compliance Officer reads nothing else in this review, these are the five developments that mattered most in 2021, why they mattered, and what they meant for a working AML program.

1. The AML Act of 2020 takes effect

Enacted on January 1, 2021 as part of the FY2021 National Defense Authorization Act, the AML Act represented the most significant overhaul of the BSA since the USA PATRIOT Act in 2001. The statute expanded BSA scope to include antiquities dealers, raised civil and criminal penalties for repeat violators, created the first FinCEN whistleblower program with awards of up to 30 percent of recovered penalties, mandated risk-based supervision, required Treasury to publish national priorities within 180 days, and authorized FinCEN to require beneficial ownership reporting through the embedded Corporate Transparency Act.

For working programs the implications were immediate. Every covered institution had to re-map its compliance program against the new statutory framework, identify which obligations applied to which lines of business, and begin a multi-quarter remediation plan. The whistleblower program in particular shifted the risk calculus around internal escalation. Institutions that had treated compliance escalation as a quiet internal matter realized that an employee with a substantiated concern now had a federal incentive to file externally if the concern was not addressed. By the second half of the year, several institutions had begun rebuilding their internal AML escalation protocols specifically with this dynamic in mind.

2. FinCEN issues the first government-wide AML and CFT priorities

On June 30, 2021, FinCEN published eight national priorities: corruption, cybercrime, foreign and domestic terrorist financing, fraud, transnational criminal organization activity, drug trafficking, human trafficking and human smuggling, and proliferation financing. Financial institutions are required to incorporate these priorities into their risk-based AML programs. This was the first time the federal government had explicitly told the industry what to focus on at a national level.

The priorities had immediate downstream effects. Examiners began structuring exam questions around how a program had operationalized each priority. Transaction monitoring teams began mapping detection scenarios to specific priority categories. Risk assessment templates that had previously used a generic risk taxonomy began adopting the FinCEN eight-priority structure as their backbone. The priorities also reframed how SAR narratives were written: examiners increasingly wanted to see clear linkage between a filed SAR and one or more named priorities.

3. Corporate Transparency Act rulemaking begins

On December 7, 2021, FinCEN issued the Notice of Proposed Rulemaking on beneficial ownership reporting under the CTA. The NPRM defined what would count as a reporting company, who would qualify as a beneficial owner, and what information would have to be reported. The proposal contemplated 23 exemptions and addressed how the database would be accessed by financial institutions and law enforcement.

For compliance teams, the CTA NPRM signaled that the underlying 2016 Customer Due Diligence rule would soon be revised to allow financial institutions to consume FinCEN's central BOI data instead of collecting it

again at account opening. The longer-term implication was the centralization of an information asset that had historically lived only in scattered account-opening files. By the end of 2021 most large banks had begun designing how they would integrate BOI data into their KYC platforms, even though the rule would not be effective for another two years.

4. NatWest pleads guilty, the FCA's first criminal AML case

NatWest Group was fined 264.8 million pounds in December 2021 after pleading guilty in October to three offences under the Money Laundering Regulations 2007. The FCA's case was the first criminal prosecution of a UK bank under those rules. The underlying facts (cash deposits totaling approximately 700,000 pounds per day from a jewellery firm in Yorkshire, accepted with controls that did not detect the pattern or escalate it) became the textbook example of why transaction monitoring needs human review on top of system alerts.

The case mattered beyond the UK. US, EU, and Asian supervisors all cited the NatWest pattern in subsequent guidance: alerts had been generated, the alerts had been disposed of, and the disposition logic was insufficient. The compliance lesson was structural. A program that runs alerts and clears them is not the same as a program that investigates. The NatWest investigation revealed that the same customer relationship had been escalated multiple times and dismissed each time, with no governance review of the dismissals. That dynamic is not unique to NatWest, and the case forced every large institution to ask whether its own alert disposition queues had the same flaw.

5. Pandemic-era fraud SAR volumes peak

FinCEN reported that SAR filings tied to pandemic relief fraud, identity theft, and synthetic identity fraud reached record levels in 2021. Across PPP, Economic Injury Disaster Loans, unemployment insurance, and federal stimulus payments, BSA filings referencing related red flags exceeded historical norms by orders of magnitude. The Treasury Inspector General and DOJ pandemic fraud task forces were both stood up at full scale during the year.

The compliance lesson was that programs designed around steady-state customer behavior failed when the entire customer base shifted overnight to digital-only onboarding and high-velocity government disbursements. Identity verification tooling that had relied on social-graph data fell behind synthetic identity attacks. Transaction monitoring tuned to retail payroll patterns produced false negatives on unemployment fraud rings. By the end of 2021, the leading institutions had moved fraud and AML closer together operationally, sharing data, sharing analysts, and in some cases reorganizing into a unified financial-crime function reporting to a single executive.

Other Material Developments

Beyond the top five, 2021 produced a set of regulatory, enforcement, and supervisory developments that did not dominate the headlines but materially affected how compliance programs are designed and tested. The items below are the ones that came up most in the program reviews and customer conversations we ran throughout the year.

OFAC reissues the Cuba and Burma frameworks

OFAC issued revised general licenses and program guidance for Cuba and Burma (Myanmar), continuing a multi-year pattern of using sanctions to respond to political crises. Compliance teams had to refresh sanctions screening rule sets, update customer outreach scripts, and re-screen historical customer files for newly-designated parties. The Burma designations following the February military coup were particularly impactful for trade-finance and correspondent-banking lines, with multiple Burmese state-owned enterprises added to the SDN list throughout the year.

Treasury publishes the National Money Laundering Risk Assessment

The 2021 NMLRA, the first since 2018, named real estate, cash-intensive businesses, professional service providers, and virtual assets as the highest-risk channels for money laundering in the US. The assessment was the analytical backbone for the FinCEN national priorities issued later in the year, and it gave program teams a citable risk taxonomy they could use when defending their risk assessment methodology to examiners.

Ransomware emerges as a top BSA threat

FinCEN issued an advisory on ransomware in November 2021 noting a sharp increase in payments routed through convertible virtual currency. The advisory directed financial institutions to file SARs that specifically referenced ransomware indicators, including the ransomware variant name where known and the cryptocurrency addresses involved. OFAC's parallel updated guidance reminded institutions that paying a ransom to a sanctioned entity is itself a sanctions violation regardless of intent.

FATF concludes the US mutual evaluation follow-up

FATF reviewed US progress against its 2016 mutual evaluation recommendations. The US received continued non-compliant ratings on beneficial ownership transparency, a finding that directly motivated CTA implementation. The follow-up also flagged areas where the US could improve information sharing between financial institutions, work that would eventually flow into the AML Act's information-sharing pilot program.

HSBC fined for UK AML failings

The FCA fined HSBC 63.9 million pounds in December 2021 for transaction monitoring deficiencies between 2010 and 2018. HSBC's case reinforced that even institutions that had previously paid record fines (the 1.9 billion dollar US settlement in 2012) remained exposed if remediation was incomplete. The finding focused on rule-based scenarios that had been generating high volumes of low-quality alerts, a pattern that would become a focus of supervisory feedback across the industry over the next several years.

Crypto enters the mainstream compliance agenda

Coinbase's April 2021 direct listing on Nasdaq, El Salvador's June adoption of Bitcoin as legal tender, and rising stablecoin issuance pushed crypto from a niche compliance topic to a board-level question for traditional

banks. The President's Working Group report on stablecoins, released in November, called for federal legislation regulating stablecoin issuers as insured depository institutions. The recommendation did not become law in 2021, but it framed the legislative debate that would continue through the rest of the decade.

FinCEN whistleblower program launches

The AML Act created a FinCEN whistleblower program modeled on the SEC's. Awards of up to 30 percent of recovered penalties shifted the risk calculus for individuals inside compliance functions. Several institutions began re-architecting their internal escalation channels, training first-line compliance staff on internal-first reporting protocols, and updating ethics-hotline routing rules to ensure compliance concerns reached a dedicated reviewer before defaulting to HR.

FDIC and OCC update BSA examination procedures

Both prudential regulators issued updates to their BSA examination manuals during 2021 to align with the AML Act's risk-based supervision mandate. The updates emphasized that examiners should focus their work on the highest-risk areas of an institution's program, rather than uniformly testing every category. Programs that could demonstrate a sound risk-based prioritization received less scrutiny on low-risk categories. Programs that could not received more.

Trade-based money laundering remains a supervisory focus

Multiple supervisory letters during the year called out trade-based money laundering as an under-detected risk, particularly in correspondent banking relationships with high-risk-jurisdiction counterparties. Programs that relied solely on trade-document review without integrated transaction monitoring received supervisory criticism, accelerating investment in TBML-specific detection scenarios.

Notable Fines and Enforcement Actions

The table below lists the headline AML, BSA, and sanctions enforcement actions of 2021, along with the regulator and the penalty amount. Where the action involved multiple regulators in a coordinated resolution, the combined amount is shown and the agencies are listed in the regulator column. This is not exhaustive: it is the set of cases that drove the most attention from compliance teams and boards during the year.

Company	Regulator	Amount	Notes
NatWest Group	UK FCA	264.8 million GBP	Criminal AML conviction, first under MLR 2007
HSBC	UK FCA	63.9 million GBP	Transaction monitoring failures 2010-2018
Capital One	FinCEN	390 million USD	Willful BSA violations in the check-cashing group
Credit Suisse	DOJ / FINMA	475 million USD	Mozambique tuna bond fraud and bribery scheme
Apple Bank for Savings	FDIC	12.5 million USD	Repeat BSA program weaknesses
ABN AMRO	Dutch Public Prosecution Service	480 million EUR	Years of CDD and SAR filing failures, settled in 2021
Deutsche Bank	Federal Reserve	Multiple consent orders	Ongoing AML and IT remediation
TD Bank (early signal)	OCC	Consent order	Early findings on AML program weaknesses that would later mature into the 2024 resolution
Julius Baer	FINMA / DOJ continuation	79 million USD	Continuation of FIFA and Petrobras-related deferred prosecution agreements
BitMEX (early)	CFTC / FinCEN	100 million USD initial	Founders later indicted, BSA-program related

Closing Note

If 2021 was about the framework being set, 2022 would be about that framework meeting a real-world shock. Russia's invasion of Ukraine in February 2022 would put every assumption in this review under stress. The institutions that came through best were the ones that had used 2021 to actually rebuild their programs against the new statute rather than treating the AML Act as a memo to read once.

That is the through-line of this series. Compliance is not a posture. It is a program. And programs need to be rebuilt regularly to keep up with the threat environment, the law, and the regulators who interpret both. Read 2022 with the question in mind: would a program built in 2021 have been ready for what 2022 actually delivered?

Dominic Suszek
Founder and CEO, Global RADAR Solutions