



Guide

Why Banks and Fintechs Need Good Compliance Programs:

Understanding Consent Orders and Their Impact

Breaking down bank consent orders and what the future of regulatory compliance holds.

cable

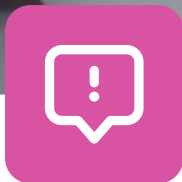
Introduction to Consent Orders

The onslaught of consent orders over the past couple of years has struck fear into many in the financial industry – but consent orders aren't necessarily a bad thing.

Yes, consent orders can come with hefty fines and remediation costs, but those are among the worst-case scenarios. Regulators' goals aren't to ruin financial institutions – quite the opposite. Their purpose is to ensure that the financial industry remains stable and strong, that financial institutions are operating safely and compliantly, and that consumers are protected.

In many cases, an institution might come out even stronger and better after a consent order because they've fixed the gaps in their own operations.

Let's break down exactly what consent orders are, what banks can expect if they receive one, and how they can use them to improve their own compliance and risk management programs.



What is a Consent Order?

First, let's break down what consent orders are.

Consent orders are a type of regulatory enforcement action. It's a binding legal agreement between a financial institution and a regulatory body to fix issues and/or deficiencies that have come to a regulator's attention. It typically outlines the deficiencies found and an implementation process for the remediation steps, which are expected to be completed within an agreed-upon timeframe.

Consent orders don't come out of the blue. They're only published once the regulators and the financial institution have already negotiated and agreed to terms on how to address any issues regulators may have uncovered. That occurs after the initial discovery, sometimes a year or more later. Prior to the negotiation process, the regulator will present any findings to the bank and give the bank the opportunity to remediate.

Any regulatory body with enforcement authority can issue consent orders to the entities they regulate, but the three key agencies are:






Office of the
Comptroller of the Currency



Consumer Financial
Protection Bureau

The main difference in consent orders comes from the scope of the agency issuing them. There is some overlap, but here is a general breakdown.

		 Office of the Comptroller of the Currency	 Consumer Financial Protection Bureau
Regulated Entities	State-chartered or OCC-chartered financial institutions that aren't members of the Federal Reserve, and all FDIC-insured banks.	National banks, federal savings associations, and federal branches and agencies of foreign banks.	Banks, thrifts, and credit unions with assets over \$10 billion, and their affiliates. The CFPB also oversees nondepository mortgage originators and servicers, payday lenders, and private student lenders of all sizes.
Areas of Regulatory Focus	Operational safety and soundness Deposit insurance Compliance within consumer protection laws	Safety and soundness Regulatory compliance	Consumer-focused financial products and services

What to Expect If Your Bank Receives a Consent Order

Even some of the healthiest, strongest banks have received consent orders.

Consent orders are unique to each bank and situation, but, generally, financial institutions have to follow these five steps:



Form an internal oversight committee.

Generally, this is made up of executives, board members, compliance officers, and perhaps legal counsel, who will review the consent orders and formulate a remediation plan.



Build a management action plan.

What are the exact steps the bank needs to take in order to remediate the issues and who is the responsible party for implementing each step?



Determine whether they need to hire a third-party consulting firm.

Sometimes, a bank will need to hire a consulting firm, either at the behest of regulators to independently monitor and verify compliance, or due to the bank's own lack of expertise in an area.



Regular reporting.

Remediation plans typically involve multiple steps, and banks need to report to regulators updates and progress on each corrective action, compliance metrics, and any audit findings.



Completion and termination.

Once the bank has satisfactorily addressed the issues listed in the consent order, the regulatory body may “terminate” the order.

Why Consent Orders Have Been on the Rise

Over the past few years, financial institutions have been getting hit with consent orders left and right, which was primarily driven by these three factors:



The change in administration

Compared to Republican administrations, Democratic administrations have generally been stricter when it comes to banking regulations.



Fintech failures and consumer harm

The collapse of Synapse this year certainly cast more light on bank-fintech partnerships, but there were numerous fintech failures and scandals (Kabbage, Chime) that likely led to increased regulatory scrutiny.



Explosion of middleware companies

One of the main pitches for many middleware companies was that it was faster, easier, and cheaper to work with them to onboard fintechs than it was to build out their own programs. Unfortunately, that also meant an additional layer between the bank and the end user, which has led to regulatory violations for some companies.

Regulation always moves more slowly than innovation. So, while some of these consent orders have highlighted real issues in bank-fintech partnerships (Sutton, Blue Ridge), a part of it is also just regulators learning how to monitor these kinds of relationships.

The Impact of Consent Orders on Banks

Remediating consent orders can be time and resource-consuming – even if a bank doesn't get hit with fines.

Cost-wise, remediation can range anywhere from thousands of dollars to millions, depending on the scope of the issue and whether a bank needs to hire additional staff and/or consultants or implement new technology.

Timewise, most of the recent consent orders have ranged from 90 to 120 days, but [S&P Global](#) believes that regulators will be pushing for much shorter time-frames.

But the biggest impact is actually on two other things: **reputation and growth**.

Not only can consent orders prevent or delay the launch of new products and services (see: [Cross River Bank](#)), it might make banks less appealing to fintechs, or cause them to completely wind down their fintech programs (see: [Blue Ridge Bank](#)).

Fintechs are big drivers of deposit growth: In 2023, they were responsible for [47%](#) of all new checking account openings. Yes, banks need to prioritize fintech compliance and risk management for their own safety, but also for the safety of their other fintech partners – and, therefore, their bottom line.

IN 2023, FINTECHS WERE RESPONSIBLE FOR

47% of all new checking account openings

Case Study: TD Bank (Worst Case Scenario)

A Brief Overview of the TD Bank's \$3 Billion BSA/AML Fine

- February 2022:** TD Bank announces it was planning to acquire First Horizon Bank, which would catapult TD Bank to becoming the 6th largest bank in the U.S.
- May 2023:** TD Bank calls off the First Horizon merger, due to increased regulatory scrutiny and uncertainty over whether the deal will get regulatory approval.
- October 2024:** TD Bank pleads guilty to money laundering charges and agrees to pay a record-breaking \$3.1 billion in penalties for breaking BSA/AML laws: \$450 million to the OCC, \$1.3 billion to FinCEN Financial Crimes Enforcement Network), and \$1.4 billion to the U.S. Department of Justice.

TD Bank should be a wake-up call for all banks and fintechs. Although TD Bank's BSA/AML violations are mainly related to internal bad actors and a culture of profits over compliance, the motivations behind these actions are familiar.

The DOJ wrote in a [statement](#) that TD Bank ignored known deficiencies in its BSA/AML policies, programs, and controls in order to prioritize the "customer experience" and a "flat cost paradigm" – maintaining the same budget despite significant increase in risk in that same period.

The Impact on TD Bank

Aside from having to pay more than \$3 billion in penalties, TD Bank is also required to establish a U.S. office specifically for remediating its BSA/AML deficiencies and will be subject to two independent monitors from FinCEN and the DOJ.

But the biggest blow is probably the [asset cap](#) placed on TD Bank's U.S. retail banking business. The bank already had to scrap its First Horizon merger and will have to indefinitely put on hold its plans to open 150 branches in the Southeast U.S. TD Bank will be subject to a much stricter approval process for new products and services.

The only other time the Fed has imposed an asset cap was on Wells Fargo back in 2018, which still remains in place and analysts estimated to have cost them \$540 billion in deposit growth.

TD Bank's BSA/AML violations and deficiencies will cost them – literally. But it has also negatively impacted their reputation and will severely restrict their ability to innovate and grow, which could include future fintech partners.

Case Study: Cross River Bank (Best Case Scenario)

On the opposite end of the spectrum is Cross River Bank, who managed to turn a consent order into a gold-star compliance program.

In March 2023, the FDIC issued a consent order to Cross River over violations in Fair Lending and deficiencies in their risk management practices, especially in relation to their fintech partnerships.

Cross River used that consent order as an opportunity to beef up their compliance and risk management programs, and to strengthen and streamline the onboarding process for fintechs.

They announced partnerships with compliance-as-a-service provider FinClusive and with fintech Current to address the risk management and fair lending issues. Most recently, in August of this year, they proactively added [three new board members](#) who have extensive experience in risk management, corporate governance, and data operations.

“They are so sophisticated in both the risk management and the infrastructure that they have built,” says Jason Henrichs, founder and CEO of Alloy Labs. “They are so good at what they do...that I know they have more demand than capacity [for more fintech partners].”

What We Can Learn from Consent Orders: Current Areas of Focus for Regulators

BSA/AML

Many of the consent orders over the past four years have been around BSA/AML. [Wells Fargo](#) recently received an OCC enforcement action over deficiencies in its internal controls and practices, like reporting suspicious activity, currency transactions, and customer due diligence. The FDIC also issued BSA-related consent orders to City National Bank and, of course, TD Bank.

Board Governance

A strong board focused on compliance and risk management will help keep an institution accountable – and compliant. Regulators have issued numerous consent orders that have required banks to strengthen their board governance, including Cross River.

What Makes a Robust Compliance Program

While it might seem like every bank working with fintechs and embedded finance companies is getting a consent order, banks can - and should - take a proactive approach to limiting the severity of those orders.

The biggest takeaway from the slew of consent orders is that banks need better compliance and risk management programs, especially as it relates to their fintech partners.

Banks need to implement adequate compliance and risk management measures that lets them appropriately monitor their fintech partners, but also need to know that, once implemented, their controls are effective at catching any breaches.

Compliance will look different for every institution, but there are two things that really make an effective and efficient compliance program:

Leveraging automation and technology

Regulators are moving toward increased oversight. Konrad Alt, managing partner at [Klaros Group](#), said that regulators establish policies first through enforcement actions before becoming incorporated into exam guidance.

That means that, eventually, increased oversight of fintech and embedded finance partners will become mandatory. Investing in automation and AI tools that help with [transaction monitoring and customer onboarding](#) will help banks manage that increased oversight without having to increase manpower.

Creating a culture of compliance

But, ultimately, effective risk management and compliance depends on strong board oversight and whether executive management fosters that culture.

Banks need to embed compliance and risk management into their everyday operations and as part of their strategic goals. Their fintech and embedded finance parties should also embody that same compliance-first spirit.

When it comes to compliance, Henrichs believes that banks need cultural and value alignment with their partners - otherwise, it could result in another Evolve/Synapse disaster.

“You need to trust that both sides are going to do whatever it takes to work out whatever happens,” said Henrichs.

Compliance Trends

The OCC just released its [Fiscal Year 2025 Bank Supervision Operating Plan](#), which highlighted areas it has identified as “material and emerging concerns.”

They have a specific section for “third-party risk,” but other relevant areas include:

Cybersecurity

Third-party risk can include cybersecurity breaches. Cyberattacks are only becoming more sophisticated, especially as the financial industry innovates.

Regulators will place particular emphasis on incident response (so, adequate monitoring and processes), backup, and operational resilience to withstand or recover from cyberattacks.

Consumer compliance

Along with continued focus on BSA/AML, the OCC also mentioned consumer compliance, including products and services provided by third-party fintechs.

That means increased attention on unfair, deceptive, or abusive acts or practices, as well as whether banks are capable of identifying and managing real-time and person-to-person payments in a timely manner.

Payments

With payments, banks need to focus on fraud prevention and risk management, especially if using new or novel delivery channels and/or third party platforms.

One area that was not directly mentioned by the OCC was reconciliation, but it remains one of the main causes of major compliance failures.

Along with accounting and bookkeeping, reconciliation is important for identifying any potential

Conclusion

The onslaught of consent orders might seem alarming, but it's also an opportunity.

Having a good compliance and risk management program is a must. Banks have seen what can happen when they don't (TD Bank) – but they have also seen how it can turn into a major boon (Cross River).

Ultimately, consent orders and enforcement actions aren't here to tear down financial institutions but rather the opposite – so banks should take the opportunity to learn from them and grow.



cable

Cable is the first Automated Compliance Testing platform that allows you to effortlessly manage compliance with automated testing of BSA/AML controls, real-time risk assessments, and proactive issue resolution—all in one platform.

To learn more, visit www.cable.tech or follow us on [LinkedIn](#).

Ready to accelerate your growth by enabling your compliance team to say YES?

Visit cable.tech/contact-us