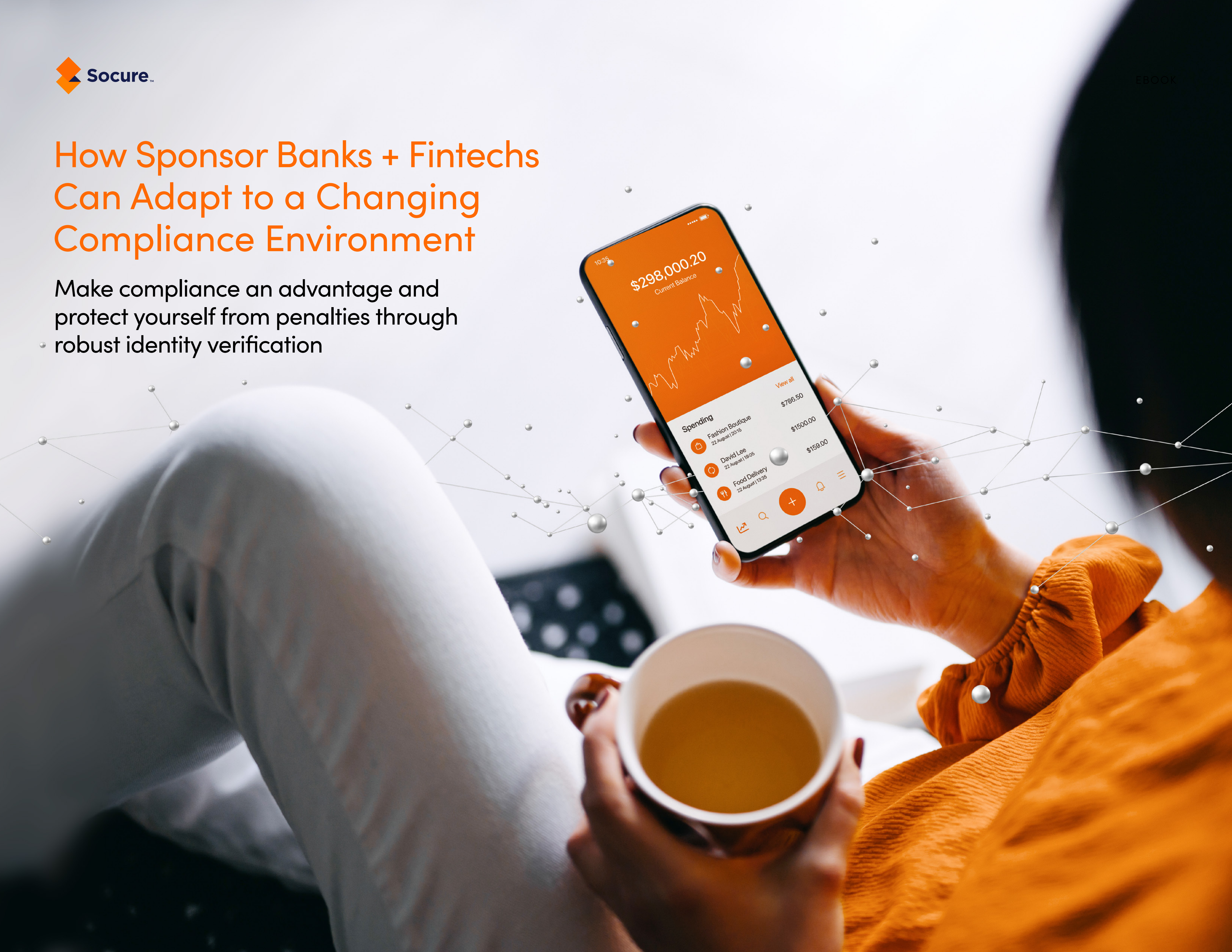
Socure

EBOOK

How Sponsor Banks + Fintechs Can Adapt to a Changing Compliance Environment

Make compliance an advantage and protect yourself from penalties through robust identity verification



Compliance's worst nightmare

It was inevitable that the explosion in the banking-as-a-service (BaaS) model would lead to more regulatory scrutiny. Through BaaS, fintechs can now offer millions of users online-only banking through sponsor banks. But over the last 18 months, financial regulators have put sponsor banks who offer banking-as-a-service (BaaS) on notice by issuing consent orders and cease and desists. 2024 is set to be just as busy.

For a BSA Officer, getting a cease and desist order from a prudential regulator can be career-altering. While the fintech revolution has opened doors for consumers, sponsor banks face mounting pressure to get compliance right. When the BaaS model was starting to ramp up, regulators didn't have a firm grasp on how to enforce laws and rarely issued adverse actions. That is no longer the case. Regulators want to see that sponsor banks are in full control over customer onboarding and due diligence.

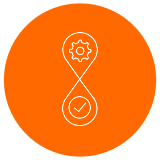
Sponsor banks have been disproportionately affected by enforcement; despite making up about 2% of U.S. banks, they accounted for 13.5% of severe enforcement actions last year. That number is steadily rising, and the impacts can be severe.[1]

Sponsor banks have hit a wall of enforcement

Regional bank collapses have changed the regulatory environment

The collapse of Silicon Valley Bank and other regional banks in 2023 became the most high-profile industry failure since the 2008 financial crisis. To fortify the system, regulators stepped up enforcement measures for capital requirements, fraud prevention, fair lending standards, and anti-money laundering/KYC regulations. Because many of the regional banks that failed were involved in fintechs and cryptocurrency, regulators naturally began to focus on the space.

Regulators are now requiring that sponsor banks have demonstrable control over who fintechs are onboarding as customers. This goes beyond basic customer identification programs (CIP) and into oversight of fraud settings, document verification, and fraud scorecards as well as behavioral transaction monitoring, Customer Due Diligence and Know Your Customer (CDD/KYC) and customer risk ratings.



Regulators are now requiring that sponsor banks have demonstrable control over who fintechs are onboarding as customers.

The ripple effects of enforcement actions

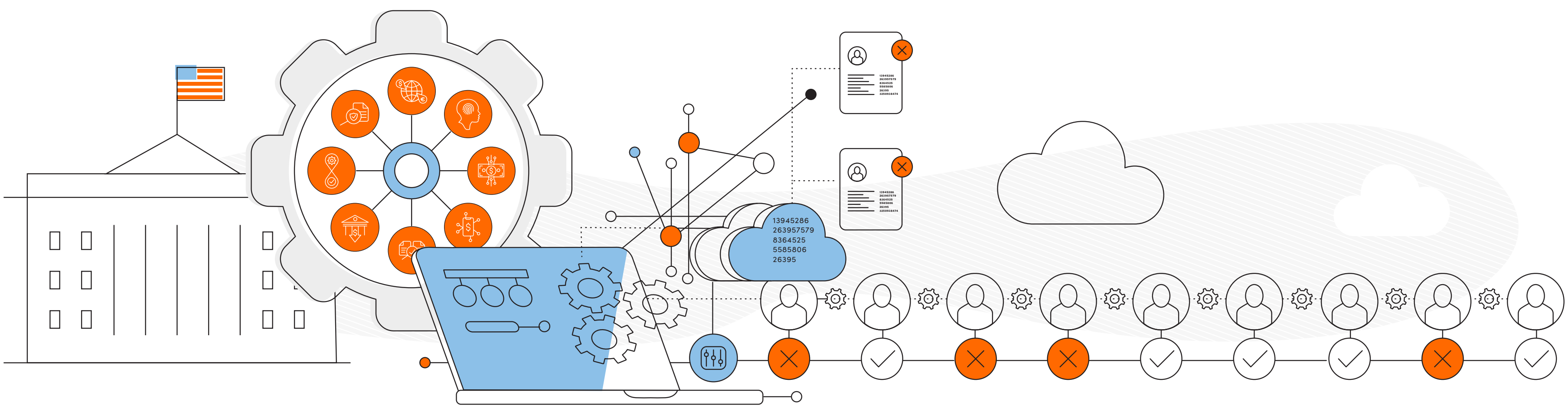
Several BaaS banks received consent orders or cease and desist orders and were forced to pay large settlements or fines. Metropolitan Commercial Bank, for example, paid a $30 million fine in Q3 2023.[2] Cease and desist orders last on average for about five years, but can extend as long as 7-10 years depending on the severity of the order and the operational impacts. There are also a host of unknown or informal enforcement actions requiring sponsor banks to demonstrate controls or pay the price. Banks are then typically obliged to voluntarily change their policies.

The raft of enforcement actions have caused reductions and even closures of BaaS programs in some cases. Some of them escalate into consent orders (a binding legal order that forces institutions to address regulatory violations, often coming with a fine). But fines and legal wrangling are just the beginning. Remediation costs can amount to 12x the original fine over the first 18 months. Enforcement actions often result in loss of new programs, vendors, reputational damage, and compromised business plans that cause long term disruption to your business.

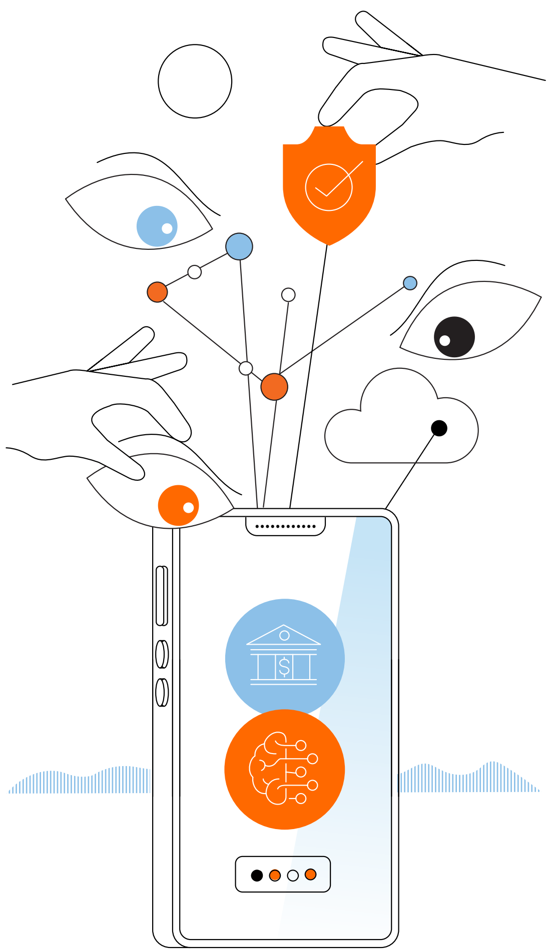
In addition, a bank under a consent order cannot make substantive changes to grow their business; new vendors, fintechs, or changes to the business typically have to first be approved by the regulators. This makes organic growth nearly impossible. But while a large bank like Chase can afford to work through enforcement issues, a sponsor bank doesn't have the same resources. **The only way to win is to comply, but in a cost-effective way.**

12X

Enforcement remediation costs can amount to twelve times the original fine over the first 18 months.



Regulatory scrutiny and the fintech model



The development of the BaaS model has left itself open to regulatory scrutiny. While fintechs offer digital and mobile services that give more opportunities for those traditionally cut out of the banking system — young people or new-to-country demographics — this increased access puts sponsor banks at greater risk of compliance issues. Though a bank provides services through the delivery channels of another company, people who use the bank's goods are still considered customers of that bank and are subject to regulations. Those regulations may have been created when a regional bank was mostly used by locals near a physical branch, but they still apply for digital-only users.

Banks prove they have controls by performing audits and reviewing policies, procedures, and controls at the fintech, but this lacks real-time data and automation. In order to demonstrate that they are actively managing risk, banks must shift to clearly show regulators they have a handle on their programs and portfolio to meet regulatory expectations. It's critical that they have full oversight of intermediary providers, which often becomes difficult when working between two separate organizations. Regulators have made it clear that the onus is on sponsor banks to demonstrate compliance. The days of relying on audit samples to display compliance are ending – it's become necessary to prove that sponsor banks have control over the process, as if the fintech were another branch of their organization.

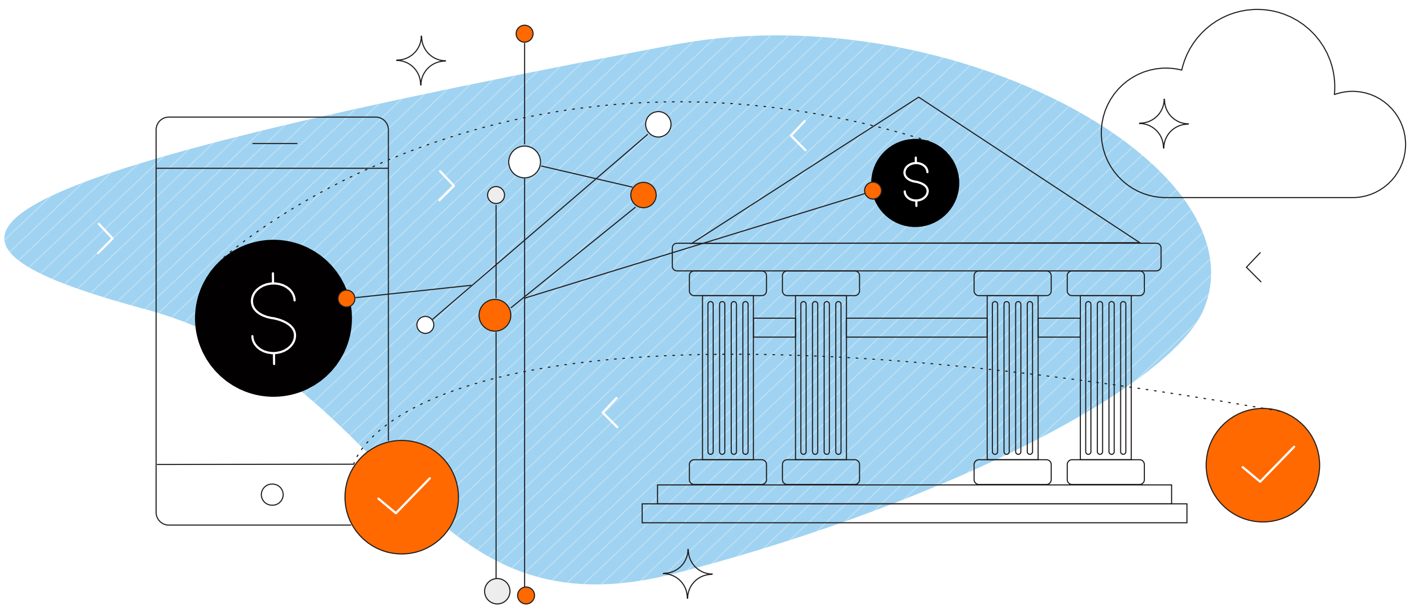
Identifying programs that fall within your risk profile has had a reaction in the BaaS world. Some programs that are creating risk for organizations are being eliminated from the portfolio. Fintechs need to be part of the solution by working closely with their banks to help them comply. Without this symbiotic relationship, sponsor banks run the risk of losing business to big banks that have established compliance practices and greater resources.

A compliance shift: From cost center to competitive advantage

In the context of increased enforcement, compliance is increasingly becoming a competitive advantage rather than a box to check. Best practices for the fintech sponsor bank ecosystems must be more open and transparent. Addressing customer risk ratings can be challenging, but there are better ways to collect information at the front end and throughout the lifecycle of the relationship.

The more disconnected the two businesses are, the more risk exists. In the most extreme example, SoFi decided to purchase Golden Pacific Bancorp and acquire its own bank charter. However, that is not a realistic scenario for most fintechs. Sponsor banks now have the responsibility to run a Customer Identification Program (CIP) for fintechs. While ensuring one entity is performing compliance checks is good for centralization, it also forces sponsor banks to invest more in security and strains internal resources.

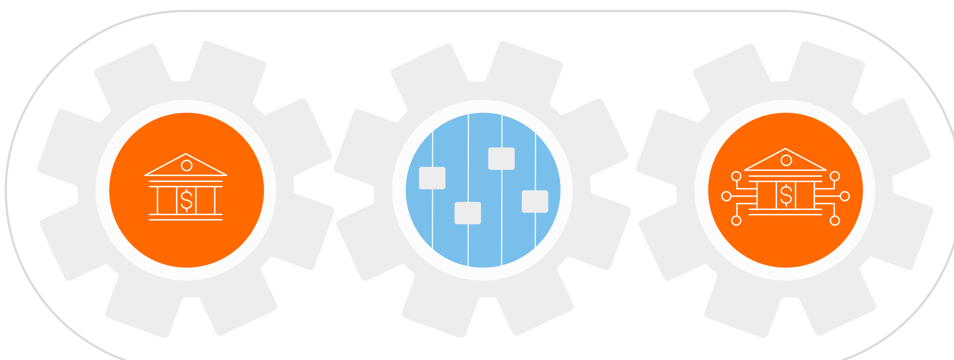
Best practices for the fintech sponsor bank ecosystems must be more open and transparent.



Wanted: a solution with clear controls and entity resolution

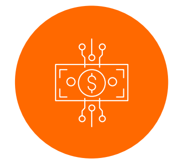
To get ahead, BaaS providers should prioritize implementing a solution that provides clear controls and oversight and centralizes compliance data for complete transparency. Banks can also explore reseller arrangements as an option to standardize fintech compliance capabilities, but may be met with challenges from prudential regulators. These institutions should discuss the arrangement with their examiner in charge (EIC) as part of their decision-making process. A bank could contract with an identity verification software provider and then license it to its fintechs. This does demonstrate control but also adds the need for additional resources at the bank. Throughout the process, all parties should continue to conduct risk assessments to identify and address vulnerabilities.

At the next level of complexity, banks can add entity resolution procedures to help identify customers that have multiple relationships. Sponsor banks also have responsibilities to stay in line with OFAC and sanctions, a feature which can be consolidated into one solution. They can also help clarify Customer Due Diligence, Enhanced Due Diligence, and customer risk rating by using specific content around the risks of the bank. PEP, Adverse Media, Human trafficking and other specific risk content can help drive better scoring and detection capabilities in the customer lifecycle. By understanding the behavior and activity across all programs, banks can help mitigate and assure their transaction monitoring programs are set to detect appropriately with the right settings.

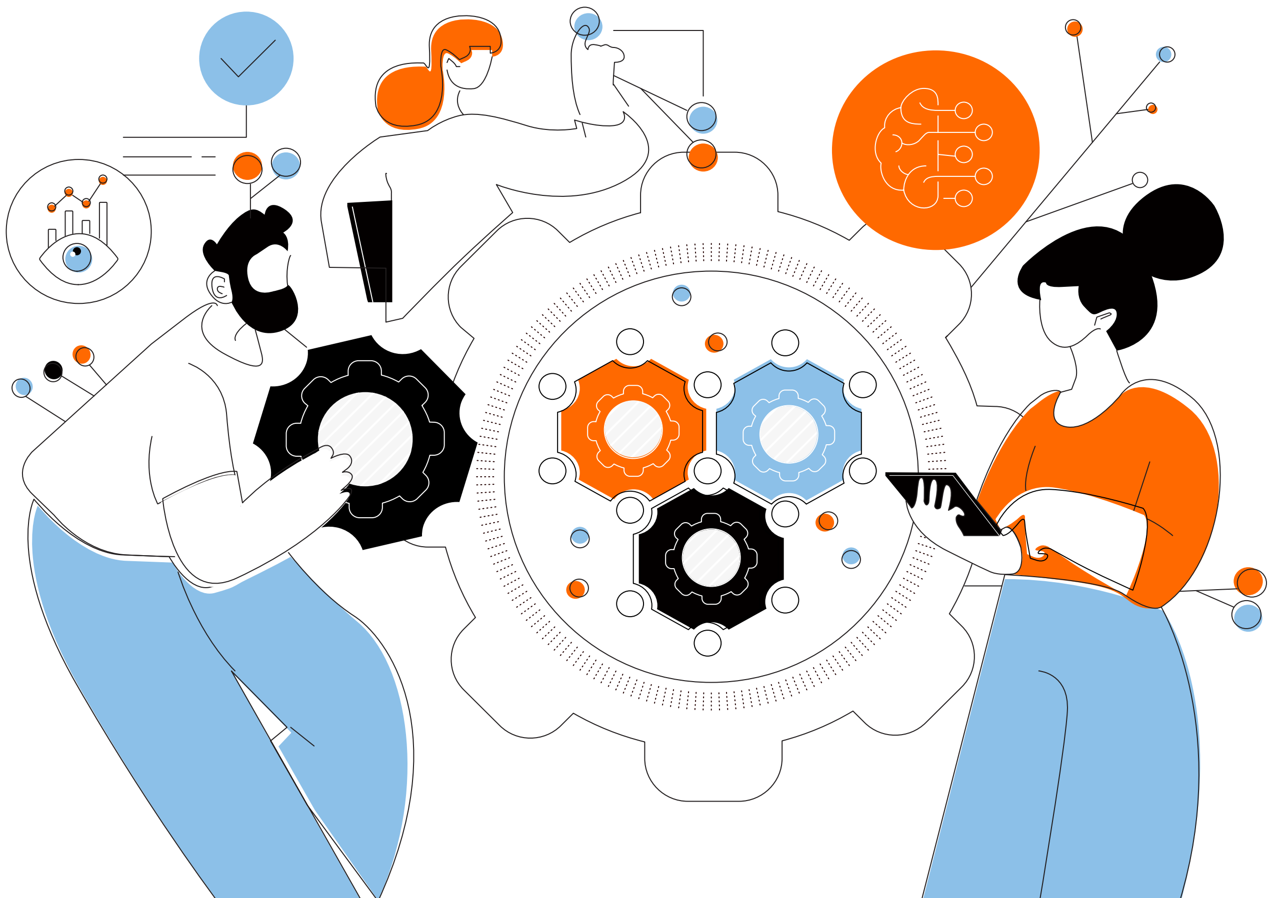


It can also be a huge step in aligning risk, policy, and process across the organization. How your IT department controls access to data and systems will all create a strong foundation for effective risk management.

In the long term, the industry should expect more enforcement actions that force fintechs and sponsor banks to make changes. Regulators have focused on using older laws like the Bank Secrecy Act as enforcement over modern digital industries, but as in the case of new beneficial ownership laws, the industry should expect updates and new regulatory guidelines.[3] Meanwhile, questions remain around what constitutes reasonable security and whether regulators will mandate protective measures or loss distribution through legislation.

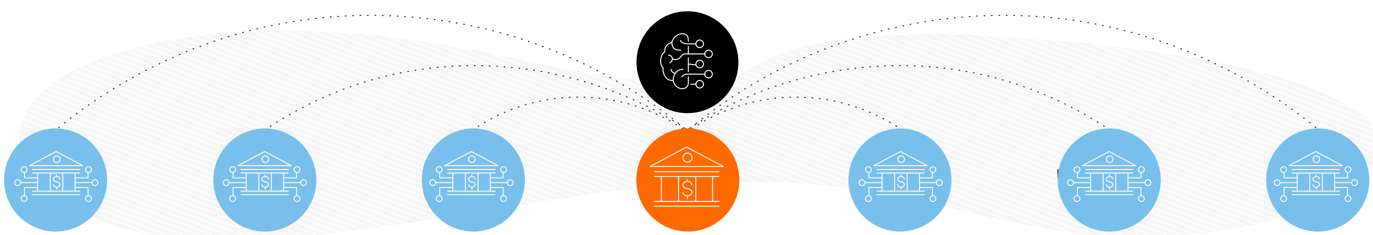


In the long term, the industry should expect more enforcement actions that force fintechs and sponsor banks to make changes.



Solution to the chaos

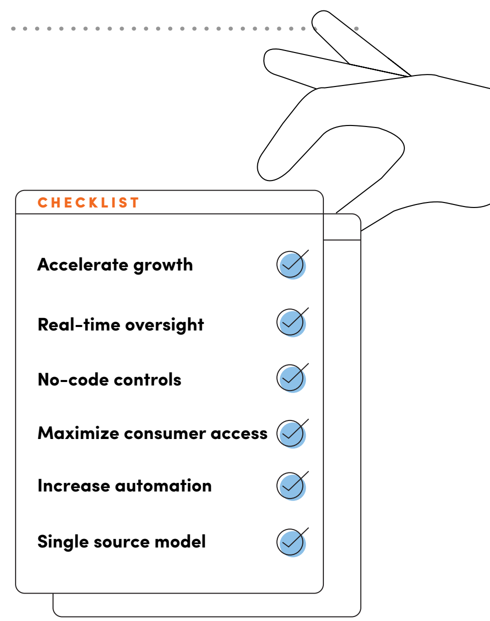
Sponsor banks are expected to prove that their controls are effective in a distributed model. These organizations will need to increase their compliance spending and keep upgrading their systems to match regulatory pressure. Managing an unwieldy stack of compliance solutions between two institutions is what's getting sponsor banks in trouble; multiple vendors with different approaches and decision standards can introduce risk in both third party risk management and oversight and control. By reducing the number of vendors, you can increase visibility across your entire portfolio to mitigate compliance risk across your BaaS partners.



With Socure's Control Center, you can achieve real-time oversight for decision logic, application flow, fraud rates, CIP/KYC approvals, watchlist cases and more with access to compliance KPIs through a single, no-code controls interface. These controls can create a collaborative environment to create demonstrable controls (and prevent enforcement actions).

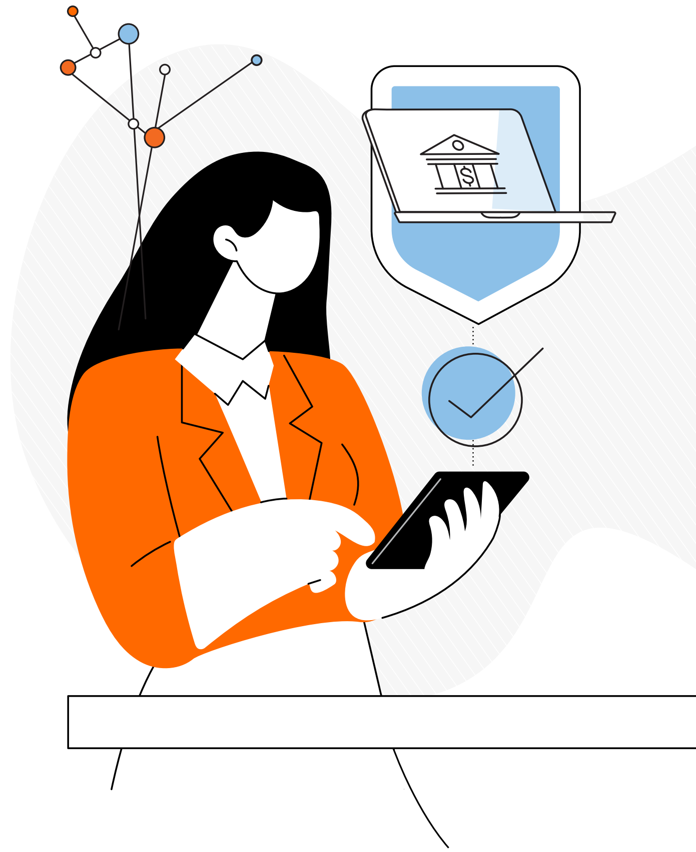
Trusted by 90% of the sponsor bank market and more than 300 fintechs, Source helps you confidently accelerate growth and stay on the right side of regulators. By enforcing consistent organizational policies paired with a complete audit trail to prove compliance, sponsor banks can enable greater control and oversight, maximum consumer access, and increased automation.

By reducing the number of vendors, you can increase visibility across your entire portfolio to mitigate compliance risk across your BaaS partners.



Powerful oversight and transparency to responsibly grow your BaaS business is possible.

LEARN MORE



Citations

1 Wang, Yizhu, and Thomas Mason. 2023. "Small Group of Banking-As-a-Service Banks Logs Big Number of Enforcement Actions." S&P Global. January 23, 2023. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/small-group-of-banking-as-a-service-banks-logs-big-number-of-enforcement-actions-80067110

2 Brasseur, Kyle. 2023. "Metropolitan Commercial Bank Fined $30M for Third-Party Oversight Failings." Compliance Week. 2023. https://www.complianceweek.com/regulatory-enforcement/metropolitan-commercial-bank-fined-30m-for-third-party-oversight-failings/33751.article.

3 Office of the Comptroller of the Currency. 2013. "Bank Secrecy Act (BSA) | OCC." Department of the Treasury. 2013. https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.

About Socure

Socure is the leading provider of digital identity verification and fraud solutions. Its AI and predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online and offline data intelligence to verify identities in real-time. Socure is the only vertically integrated identity verification and fraud prevention platform with both IAL-2 and FedRAMP Moderate certifications, delivering advanced levels of assurance and the highest standards for security and compliance. The company has more than 2,000 customers across the financial services, government, gaming, healthcare, telecom, and e-commerce industries, including four of the five top banks, the top credit bureau and more than 400 fintechs. Organizations including Chime, SoFi, Robinhood, Gusto, Public, Poshmark, Stash, DraftKings, and the State of California trust Socure for accurate and inclusive identity verification and fraud prevention. Learn more at socure.com