CISIVE

Navigating Background Screening Regulations:

A Guide for Regional Banks

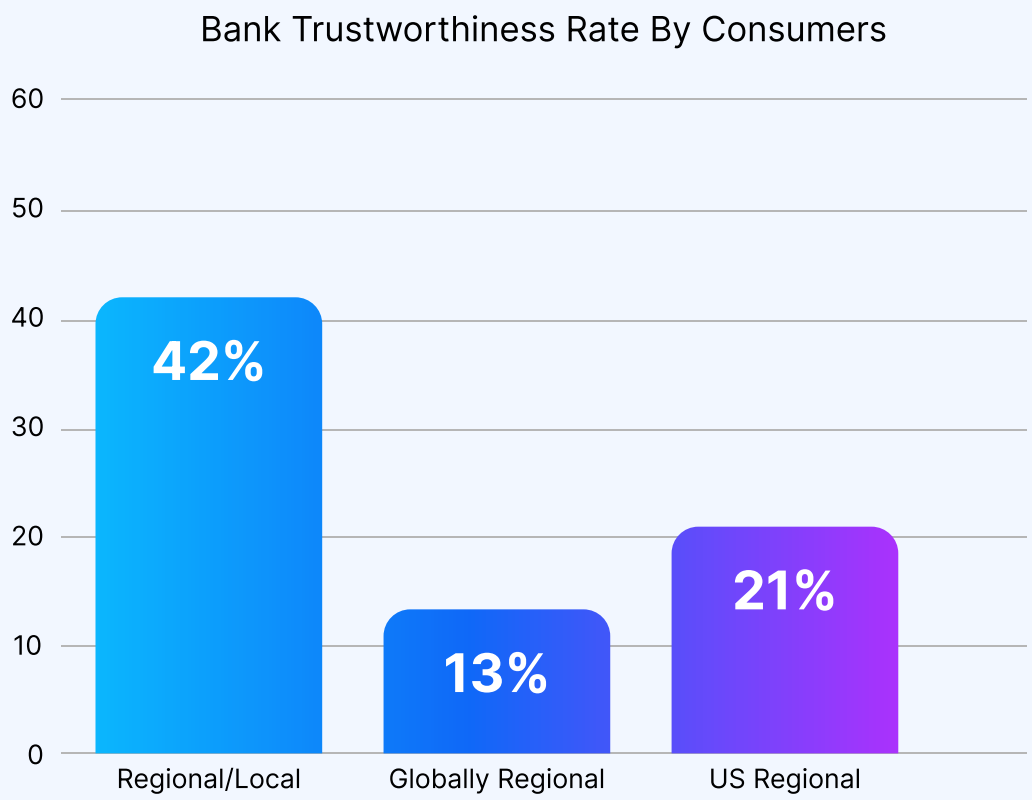
Table of Contents

Introduction

Regional banks play a vital role in the financial ecosystem, offering personalized service and deep ties to the communities they serve. While these institutions may not have the scale of national banks, they possess a unique opportunity to build and maintain strong, local relationships and foster a sense of trust. Trust is the cornerstone of any successful bank, and regional banks in the U.S. are significantly more trustworthy than global averages, according to research from Kantar.

A survey found that nearly half (42%) of banking customers rated regional banks as trustworthy.

On average, globally, 13% of respondents place high trust in regional financial institutions. In the U.S., however, that number climbs substantially to 21%.



Trust matters, especially for regional banks. Ensuring you hire only the best talent is a key component of building trust — and that starts with the background check. Imagine discovering a senior employee at your bank has a criminal record that slipped through the cracks due to inadequate screening. Such an oversight could lead to devastating consequences — not just in terms of legal repercussions but also in the erosion of trust within your community.

As HR leaders, you understand that background screening is more than just a checkbox — it's a critical element of your risk management, compliance, and talent strategy. This guide explores the unique challenges regional banks face in the background screening process and offers practical solutions to help you navigate this complex landscape.

Navigating Regulatory Complexity

Let’s begin by laying the foundation. The first and most crucial step in implementing a compliant background screening program for financial services is understanding the regulatory requirements that govern the background screening process and regulations specific to hiring in financial services.

Starting with regulatory understanding ensures that every subsequent decision aligns with legal obligations, protecting your bank from severe penalties and reputational damage.

Fair Credit Reporting Act (FCRA)

The Fair Credit Reporting Act (FCRA) sets stringent guidelines for collecting, using, and disposing of consumer information during background checks. To maintain compliance with the FCRA, regional banks must adhere to several critical obligations throughout the hiring process. First, you are required to provide candidates with a clear disclosure that a consumer report will be used for employment purposes. Then you must obtain the candidate's explicit written consent before conducting the background check. This transparency ensures that candidates are aware of how their information will be used.

If a background check reveals information that could lead to a decision not to hire, you must follow a two-step adverse action process. Initially, a pre-adverse action notice, including the consumer report and a summary of the candidate's rights under the FCRA, must be provided to allow the candidate to review and dispute the findings if necessary.

If the decision to deny employment is upheld, a final adverse action notice must be issued, detailing the decision and providing contact information for the consumer reporting agency.

In addition to these steps, employers are responsible for the accuracy of the information used in hiring decisions. If a candidate disputes the report's accuracy, you must promptly reinvestigate and correct any inaccuracies. Furthermore, regional banks must properly dispose of consumer information after use, ensuring that sensitive data is protected against unauthorized access.

By diligently following these guidelines, regional banks can navigate the complexities of the FCRA, reduce legal risks, and maintain candidate trust throughout the hiring process.

General Data Protection Regulation (GDPR)

Maintaining General Data Protection Regulation (GDPR) compliance in the background screening process is essential for regional banks operating within or interacting with the European Union. GDPR imposes strict requirements on how personal data is collected, processed, and stored, making it crucial for banks to prioritize data privacy. To comply, you must ensure that candidates are fully informed about the data being collected and the purpose behind it, and you must obtain explicit consent before proceeding with any background checks. Additionally, you'll need to implement robust data security measures to protect personal information from breaches or unauthorized access.

Furthermore, regional banks must ensure that the transfer of personal data across borders is handled carefully, particularly when using third-party vendors or conducting international background checks. This includes evaluating the adequacy of data protection measures in non-EU countries and establishing appropriate safeguards, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). Regular audits and reviews of data processing activities are also vital to ensure ongoing compliance with GDPR. By integrating these practices into your background screening processes, you can effectively mitigate legal risks at your regional bank and uphold the highest standards of data privacy.

California Consumer Privacy Act (CCPA)

Regional banks operating within the state of California are subject to the California Consumer Privacy Act (CCPA). If you're hiring in California, you must prioritize transparency and data protection in background screening procedures to achieve CCPA compliance during the hiring process. Under the CCPA, banks must inform job applicants about the specific types of personal data being collected and the reasons for their use. This includes providing clear notice before any data collection takes place. Additionally, you are required to honor applicants' rights to access, delete, or opt out of the sale of their personal information.

To maintain compliance, banks should implement systems that allow them to process and respond to these requests promptly and securely. Regular audits of data practices and comprehensive training for HR and legal teams are also essential to ensure ongoing adherence to CCPA standards. Safeguarding personal information against unauthorized access is critical, as non-compliance can lead to severe financial penalties and reputational harm.

Ban the Box Laws

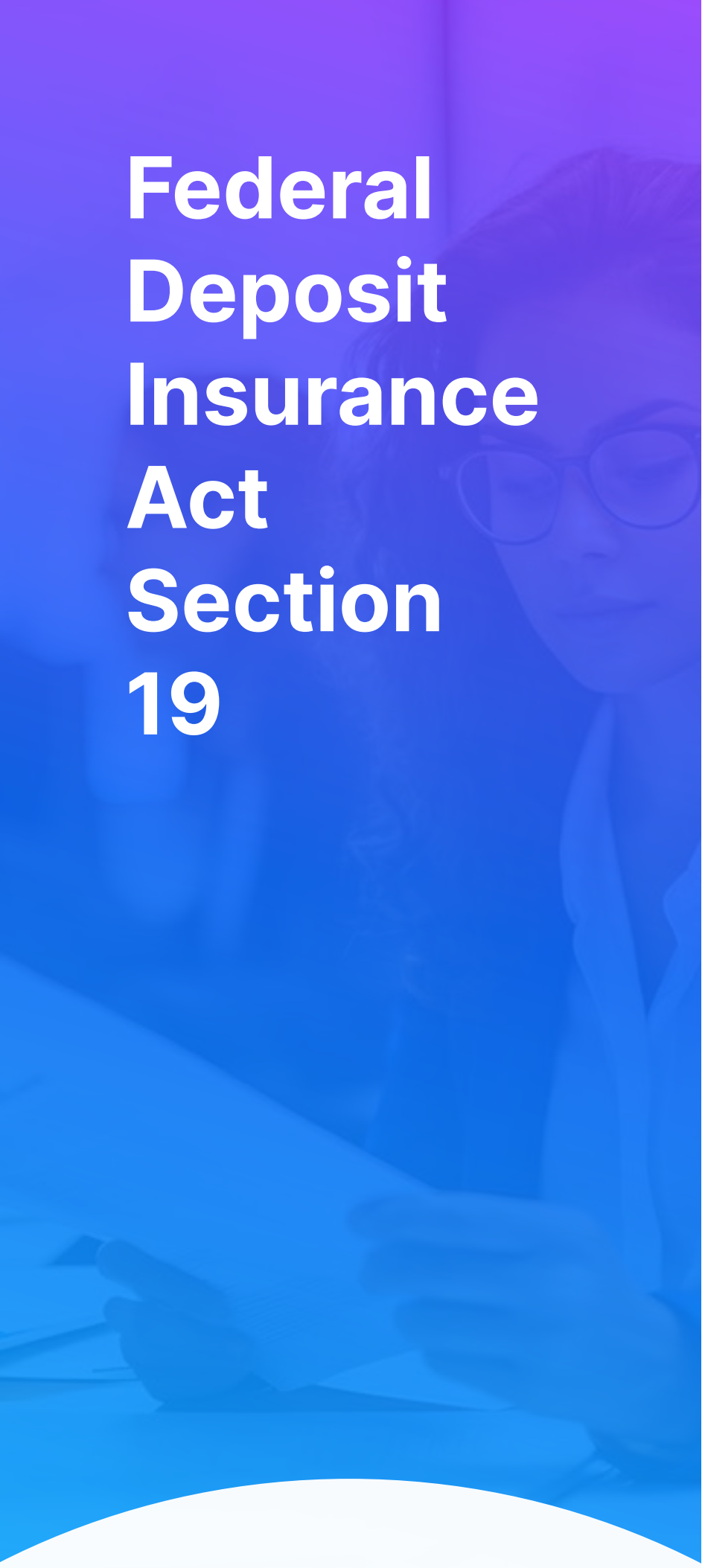
To maintain compliance with Ban the Box laws during the background screening process, regional banks must carefully manage the timing and use of criminal history inquiries. Ban the Box laws typically prohibit employers from asking about criminal records on job applications, requiring you to wait until later in the hiring process to conduct background checks. This approach allows candidates to be evaluated on their qualifications first, without the stigma of a past conviction influencing the initial hiring decision.

For regional banks, it's crucial to ensure that criminal history inquiries are conducted in compliance with both local and state regulations. This may involve postponing the background check until after a conditional job offer has been made.

Additionally, if a criminal record is found, banks must provide the candidate with an opportunity to explain the circumstances and consider factors such as the nature of the offense, its relevance to the job, and the time that has passed since the conviction.

Regular training for HR staff and collaboration with legal counsel can help ensure that these laws are followed correctly, minimizing the risk of legal challenges while promoting fair hiring practices. By adhering to Ban the Box laws, regional banks can contribute to reducing employment barriers for individuals with criminal histories while maintaining a compliant and fair hiring process.

Federal Deposit Insurance Act Section 19



Failure to comply with Section 19 can result in hefty fines

$1 million

per day or imprisonment

However, there are certain convictions that could prohibit individuals from serving in certain roles at a financial institution. Section 19 of the Federal Deposit Insurance Act, for example, prohibits individuals convicted of crimes involving dishonesty, breach of trust, or money laundering from participating in the affairs of an FDIC-insured institution without first obtaining written consent from the FDIC. This rule applies broadly to any employee, director, officer, or consultant involved in a bank's management or operational activities.

For employers, compliance with FDIC Section 19 is non-negotiable and requires a proactive approach to background screening. Employers must conduct thorough background checks to identify any disqualifying criminal convictions before hiring or retaining individuals in roles that involve significant decision-making or fiduciary responsibilities. This due diligence is essential to avoid unauthorized participation that could lead to severe penalties.

Failure to comply with Section 19 can result in hefty fines — up to $1 million per day — or imprisonment. Therefore, financial institutions must have robust screening processes to ensure all potential and current employees comply with this regulation. This includes continuous monitoring and re-screening as necessary, particularly if an employee's role changes or new criminal records surface.

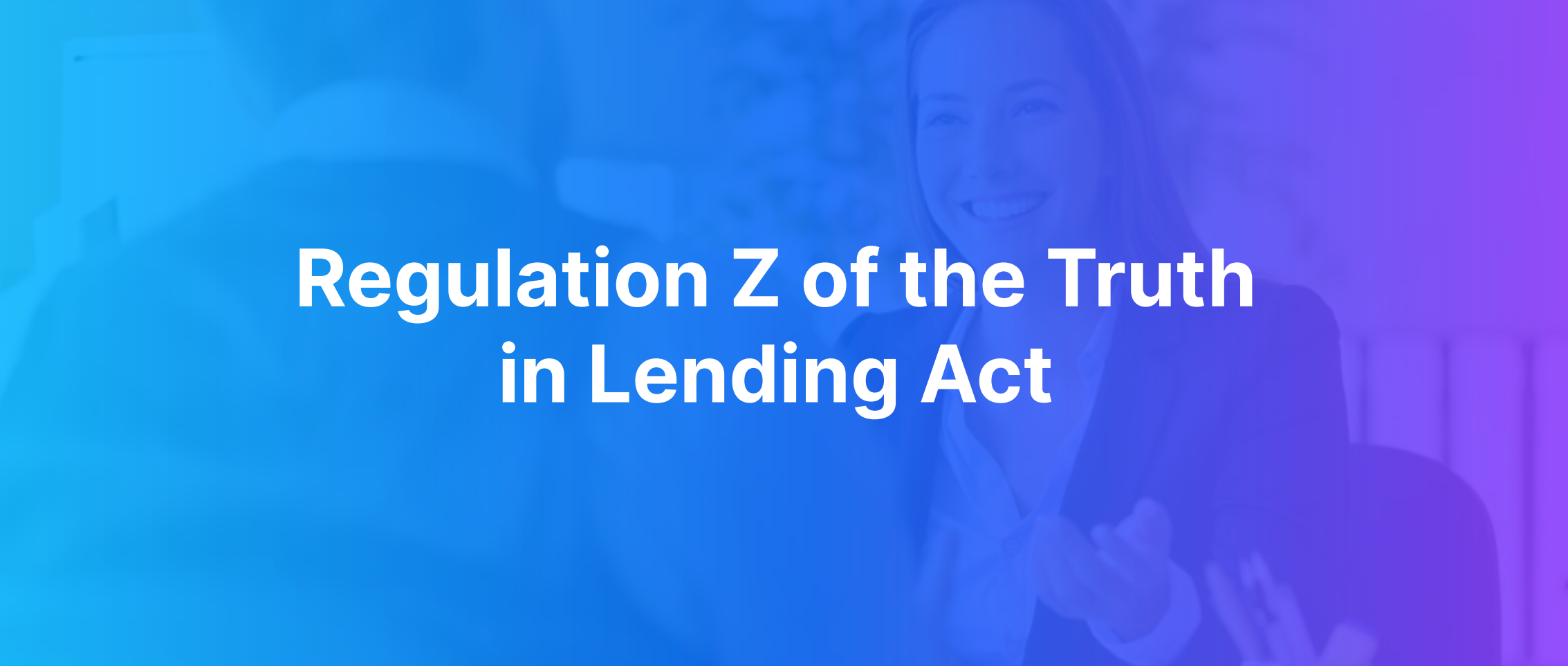
The Secure and Fair Enforcement for Mortgage Licensing (SAFE) Act

The Secure and Fair Enforcement for Mortgage Licensing (SAFE) Act is a federal law requiring individuals responsible for originating mortgage loans to be registered or licensed. This law applies to employers in the financial services sector, specifically those involved in residential mortgage loan origination. Under the SAFE Act, any employee who takes a residential mortgage loan application, offers or negotiates terms, or assists a consumer in obtaining a mortgage must be registered with the Nationwide Mortgage Licensing System and Registry (NMLS).

For financial services employers, any employee who performs these functions must meet the SAFE Act's requirements. Employers are responsible for ensuring their mortgage loan originators (MLOs) are properly registered and maintain their registration status.

This includes conducting background checks, ensuring the employee meets education requirements, and regularly updating their registration in the NMLS.

To comply with the SAFE Act, financial services employers should have a clear process for identifying which roles within the organization require registration and ensure that these employees know their obligations under the law. Regular audits and ongoing training can help maintain compliance, and employers should work closely with legal counsel to navigate any complexities related to the Act. Employers should develop written policies establishing processes for reviewing employee criminal background reports, taking appropriate actions, and maintaining records of these reports and actions.



Regulation Z of the Truth in Lending Act

Regulation Z, part of the Truth in Lending Act (TILA), mandates that financial services employers conduct thorough background screenings for individuals classified as “loan originators.” These roles involve handling loan applications, negotiating terms, and offering consumer loans, making them critical in ensuring transparency and fairness in lending practices.

Employers must conduct criminal background checks through the Nationwide Mortgage Licensing System and Registry (NMLSR) or through a law enforcement agency or commercial service if the individual is not registered. Additionally, employers are required to obtain a credit report from a consumer reporting agency to assess the loan originator's financial responsibility. They must also collect information from the NMLSR regarding any administrative, civil, or criminal findings against the loan originator; if the individual is not registered, this information must be gathered directly from the person.

To comply with Regulation Z, you must establish written policies outlining the procedures for conducting these background checks, reviewing the results, and taking appropriate actions based on the findings. These policies should also ensure that all records of the background checks and any actions taken are meticulously maintained. This process is essential for maintaining compliance with federal regulations and safeguarding the institution and its customers by ensuring all loan originators meet the necessary regulatory standards.

Financial Industry Regulatory Authority (FINRA) 3110

FINRA Rule 3110 requires financial services firms to carefully supervise their employees, particularly those working as brokers, investment advisors, or in other securities-related roles. The goal is to ensure that these professionals follow legal and ethical standards. Firms must conduct thorough background checks on these employees to comply with this rule. This includes checking for criminal records, past regulatory violations, and other relevant issues that could affect their ability to handle clients' investments responsibly.

These background checks are crucial for identifying potential risks and ensuring that only qualified, trustworthy individuals are employed in these sensitive roles. You must also create and maintain written policies that outline how these background checks will be performed, how the results will be reviewed, and what actions will be taken if issues are found.

By having these procedures in place, your institution can protect both your clients and your reputation.

Rule 17a-3(a)(12) of the Securities Exchange Act of 1934

Rule 17a-3(a)(12) of the Securities Exchange Act of 1934 requires financial services firms, including broker-dealers, to maintain up-to-date records for their “associated persons.” This rule applies to individuals involved in securities activities, such as brokers and financial advisors. Employers must collect detailed information, including a questionnaire or employment application that documents any arrests, indictments, and the outcomes of those legal issues, particularly for crimes related to securities, banking, fraud, and similar offenses.

To comply, your institution must conduct thorough background checks to gather and verify this information, ensuring that any past criminal activity is accurately recorded. This helps you assess your employees’ suitability for roles involving significant financial responsibilities.

Ensuring Accuracy & Consistency

The risks associated with inaccuracies in background checks are amplified for regional banks. Errors in public records, outdated databases, and mistaken identity can lead to unfair hiring decisions, legal challenges, and significant reputational damage. Given the critical nature of roles in your institution, the margin for error is slim.

To mitigate these risks, it's essential to adopt a strategic approach to accuracy and consistency in your background screening process. Leveraging advanced verification technologies and maintaining partnerships with reliable screening providers can help ensure the integrity of your data. Additionally, continuous monitoring and regular updates to your screening processes are key to maintaining accuracy and protecting your institution's reputation.

Your institution's legal counsel and an informed vendor partner can help tremendously in this effort.

Enhancing the Candidate Experience

Trust matters, especially for regional banks. Ensuring you hire only the best talent is a key component of building trust — and that starts with the background check. Imagine discovering a senior employee at your bank has a criminal record that slipped through the cracks due to inadequate screening. Such an oversight could lead to devastating consequences — not just in terms of legal repercussions but also in the erosion of trust within your community.

As HR leaders, you understand that background screening is more than just a checkbox — it's a critical element of your risk management, compliance, and talent strategy. This guide explores the unique challenges regional banks face in the background screening process and offers practical solutions to help you navigate this complex landscape.

Leveraging Technology Integrations

Technology plays a crucial role in modern background screening, but for regional banks, integrating these solutions with existing HR and IT systems can be challenging. Ensuring compatibility and managing cybersecurity risks are key concerns.

Automation offers significant advantages in terms of efficiency and accuracy, particularly for banks with limited HR resources. However, the cost of implementing automated solutions can be a barrier. For regional banks, carefully evaluate the ROI of automation and consider phased implementations to spread out costs.

As technology continues to evolve, staying ahead of trends in background screening will be critical for maintaining compliance and operational efficiency. By investing in scalable, future-proof solutions, regional banks can ensure that HR operations remain resilient and adaptable to changing regulatory landscapes.

Looking Forward

As the financial services landscape evolves, so do the challenges and opportunities associated with background screening. Emerging technologies such as digital identity verification, blockchain, and AI-driven tools are reshaping how regional banks approach compliance. Working with the right vendor partner offers new ways to streamline processes, enhance accuracy, and reduce risk. These developments promise greater efficiency and provide a proactive approach to managing the increasingly complex regulatory environment.

For regional banks, staying ahead of these trends is crucial. By refining your background screening program and working with your vendor partner to integrate cutting-edge tools, you can help make sure your institution remains compliant, resilient, and trusted in the eyes of regulators and the communities you serve.

However, navigating this rapidly changing landscape requires more than awareness. It demands action. The concepts this guide outlines provide a solid foundation, but the key to success lies in ongoing commitment and adaptability. Your bank's reputation, security, and operational success depend on it.

To enhance your background screening program and address your institution's unique challenges, consider partnering with experts who understand the intricacies of financial services compliance.

> Schedule a call with one of Cisive's background screening specialists today to discover how you can enhance your program, protect your reputation, and build even stronger ties with the communities you serve.

Balancing Time & Costs with Strategic Priorities

Time is a critical factor in the hiring process, especially in a competitive talent market. However, the need for thorough background checks can create delays that put you at a disadvantage. For regional banks, balancing the need for efficiency with the demands of comprehensive screening is a unique challenge.

The resource-intensive nature of background screening can strain smaller banks' budgets, particularly when compliance with complex regulations is required. However, there are scalable solutions available that allow you to maintain high standards without breaking the bank. Streamlining your background screening process through automation and strategic outsourcing can help you manage costs while ensuring thorough results.

Background screening isn't just a compliance requirement. It's a strategic investment. By optimizing your screening processes, you can reduce the time-to-hire, enhance the quality of your hires, and ultimately improve your institution's overall performance. Calculating the ROI of these processes can help you make a strong business case for the necessary resources and technology investments.

Work with your vendor partner to understand the true value of your current background screening program, and to make the case for investing resources in more advanced screening processes.

CISIVE

Talent Intelligence To Upskill Your Workforce

Cisive.com | 888-575-9959