First Advantage
A Symphony Technology Group Company

How to Conduct Successful Background Checks on Existing Employees

Strengthening Security from Within

Table of Contents

Introduction

Screening your company's existing workforce can be a critical component in your overall security plan. But the process is far from simple—and is often intimidating. Learn from one company that has navigated the complexities, and consider their strategies to help you plan the process.

Pre-employment background screening is now considered a standard practice in Corporate America. Very few companies, however, are crossing the threshold to conduct screens on their existing workforce. It's a complex endeavor, and to be successful, companies need to walk a fine line between addressing legitimate business and security risks and not alienating employees along the way.

3-Phased Approach to Create a Win-Win Rescreen Plan

1. Get executive buy-in and create a plan
2. Over communicate the intent and process
3. Roll-out the program from the top down

As companies undertake the huge challenge of background screening its existing workforce, this guide outlines the best practices using an example of how one company did so successfully.

> *"As the head of human resources (HR) for the U.S., I can tell you that this initiative, without question, could have been perceived as the most negative program that we potentially could have ever rolled out," said the Senior Vice President (SVP) of HR. "We had to navigate each decision carefully, with the utmost discretion at every turn, and ensure we designed a multi-faceted and comprehensive employee communications plan."*

Therefore, to create an atmosphere of sharing and communication to minimize employee concern, this company developed a four-phased approach to create a win-win for the company and the employees.

Phase I: Pre-Launch Process Design

Formulate the Initial Process Design

To kick off the employee-screening initiative, the company formed a core design team that consisted of senior members from HR, Legal and Security. Together, this team created the guiding principles for the process design, which in turn, drove the roll-out and employee education efforts. The fundamental design principles were as follows:

Around 30% of organizations rescreen

Not many public, independent surveys have been completed around why organizations rescreen. SHRM (Society for Human Resource Professionals) conducted a survey in 2007 identifying who is rescreened and why:

A position within the organization warrants it
48%

A position promotion
30%

All positions—standard practice one year after hiring
4%

Varied other reasons
18%

- **Principle #1:** Make a plan to over-educate and over-communicate with employees.
- **Principle #2:** Assume positive intent on the part of the employees and don't rush to judgment.
- **Principle #3:** Keep the entire process simple, easy to understand, and as short as possible.
- **Principle #4:** Ensure confidentiality throughout the process.

The team also defined the background checks themselves—including a review of criminal convictions, such as trust-related crimes of deceit, dishonesty or fraud (e.g., theft, embezzlement). Thus, the team decided to screen for identity authentication, clearance against the Office of Foreign Asset Control (OFAC), and national, multi-state and county criminal record searches. Together these checks would cast a wide net across the U.S.

Get Executive Buy-In

Once the process design began taking shape, the three-person steering committee sought buy-in from all C-level managers in the U.S. During a series of executive briefings, the team presented the proposed process design, and took the time to help these managers understand the process, the implications and the roll-out strategy.

Once the process was designed and senior executives were on board, the design team started writing policies, procedures and general parameters around program roll-out and employee communication. The steering committee then turned the program over to an implementation team—now tasked with execution across the business.

This implementation team was cross-functional in makeup—and consisted of managers from a wide diversity of roles, including:

- Human resources (generalists)
- HR information systems
- Security
- Information technology
- Legal
- Representatives from the background screening provider
- Internal communications

Searches Commonly Selected for Rescreening By Industry

Some regulated industries such as healthcare, transportation, or financial services require rescreening. Others are selecting to rescreen—recognizing the value to verifying current status.

Education:
- Sex Offender Registries
- National Criminal

Healthcare:
- FACIS (Fraud and Abuse Information Control System)
- National Criminal Registries
- Abuse/Occupational Registries

Non-Profit
- Sex Offender Registries
- National Criminal

Financial
- National Criminal
- Financial Sanctions

Retail
- National Criminal

Staffing
- National Criminal

Transportation
- MVR (Motor Vehicle Record)
- National Criminal

Conduct Pilot Programs

Before launching the program company-wide, the company launched a series of pilot programs, to make sure the processes and decision logic were sound. The first pilot screened a small group of senior HR leaders and the implementation team. Once that was done—and minor corrections made—the team ran a larger pilot, which screened all the U.S. leaders in HR, legal and security departments.

> *"We thought it was important to do these groups first, to demonstrate to employees that the individuals who could potentially be doing investigations, viewing data or making recommendations on potential employee actions had already gone through this process themselves," said the VP of the implementation team leader.*

Phase II: Process Roll-Out

Once the pilot program concluded, the company was ready to start screening the general employee population. Because of the sheer size of the organization, however, screening all 6,000 employees at once was simply not feasible.

> *"The process of conducting, reviewing and evaluating employee results takes time—and thousands of results coming back at once would have caused a major process bottleneck," explained the VP of the implementation team leader.*

Thus, the company wisely decided to "batch" employee groups by business divisions and buildings—conducting around 300 employees at a time. Here's a step-by-step glimpse of the how the actual process worked:

The Employee Screening Process, At a Glance

Train Employees – Communicate the plan details using online announcements, emails, and face-to-face meetings.

Get Employee Consent – In accordance with the Fair Credit Reporting Act and other applicable state laws, employees had to give permission to have their background screened.

Confirm Employee Identity – Then, they had to answer questions about their personal identity to confirm that they are who they say they are.

Collect Employee Declarations – Employees then were asked to disclose, in accordance with the applicable state laws, convictions other than minor traffic violations going back seven years.

Get Employee Consent

↓

Confirm Employee Identity

↓

Collect Employee Declarations

↓

Conduct Batch Testing

↓

Review Audit Files

↓

Share Results with Employees

↓

Conduct Any HR Investigations

↓

Close Out the Files

Conduct Batch Testing – These screens got processed in batches of 300 at a time. Several days later, the reports would come back. All "clean" reports, meaning no issues with the verifications or criminal checks reported, were closed immediately—with no additional action taken. Any reports indicating that there was an issue with the verifications, or a criminal conviction, went into an "audit file" for subsequent review by a two-person core review team (Senior VP, HR and Chief Security Officer).

Review Audit Files – Every week, the two person review team met and worked through the audit file. Many times the issues raised were cases of a mistaken identity or an error in the public record. Each incident was evaluated and viewed in light of the employee declaration, the nature of the conviction, and the position held by the employee among other factors.

> *"If we were to find a situation where we had to make an employment-related decision, we would work with our legal counsel and the unit head for the employee's business unit. After educating them on the situation, the Chief Security Officer and I would then recommend the action we think might need to be taken—anything from separating the employee from the company to changing the employees' roles and responsibilities," said the SVP of HR.*

Share Results with Employees – A copy of the background screen itself was delivered to each employee within a day of being submitted to the review team.

This added value in two ways. The short turnaround time relieved some anxiety on the part of employees. Plus, having a copy of their individual report enabled them to identify false-positive results or cases of potential identity theft. To help them read and interpret their reports, the company featured a sample report on the intranet site, along with a full explanation on how to interpret it.

Conduct Any HR Investigations – Inaccuracies or inconsistencies in employees' records were also sent electronically to an HR team member, who would then, in concert with the employee, help clarify the facts surrounding the events.

Close Out the Files – Once all items on the audit reports were finalized, the files were closed. If any adverse action were to be taken, FCRA and applicable state law process were followed.

> *"Aside from the employee himself or herself, generally, the only other people that saw a person's background report was the SVP of HR and myself," explained the Chief Security Officer. "The whole review process was very controlled. The results were not for publication, and were not going in an employee's manager's file. Our main goal was to view the results and close out issues as soon as possible."*

"If we were to find a situation where we had to make an employment-related decision, we would work with our legal counsel and the unit head for the employee's business unit. After educating them on the situation, the Chief Security Officer and I would then recommend the action we think might need to be taken—anything from separating the employee from the company to changing the employees' roles and responsibilities."

> *"Over communicating the process and our overall objective helped relieve a lot of employee's concerns," added the SVP of HR. "Understandably, they weren't quite sure who was going to see what, where the data would be going, how it would be stored, and if it was going to be held against them for future career advancements."*

Ironically, some of the items found actually ended up being beneficial to employees. Individuals have found some isolated cases of identity theft, as well as cases of multiple users sharing a social security number. The company offers follow-up resources to help employees work through these issues.

Keeping Up Employee Morale: Communication is Key

One of the reasons this company's employee screening initiative has had minimal impact on employee morale was summed up in one word: communication.

> *"I just don't believe that you can over-communicate with this type of process," said the SVP of HR. "The more a company can transparently communicate with its employees, the better off it will be. We knew that employees may consider this a huge affront to their personal privacy—and we had to overcome this challenge with communication—explaining what we were doing, the business reasons behind doing it, and our commitment to confidentiality."*

To do that, the implementation team used a variety of communication methods to inform people of the initiative and process, including:

- Introductory letters
- Face-to-face executive briefing meetings
- Town hall-style employee meetings, held just prior to commencing the screening process in a new business unit
- A dedicated intranet site, containing:
    - A detailed process map
    - Videos
    - Frequently asked questions
    - Information on how to read a background screen report
    - Articles of interest
    - Links to internal and external resources that can help resolve data inaccuracies
    - Links to organizations that could help resolve matters surrounding identity theft

"I just don't believe that you can over-communicate with this type of process," said the SVP of HR. "The more a company can transparently communicate with its employees, the better off it will be. We knew that employees may consider this a huge affront to their personal privacy—and we had to overcome this challenge with communication—explaining what we were doing, the business reasons behind doing it, and our commitment to confidence."

> *"We had to make sure to send the message loud and clear that this was not a punitive process and that our employees would be given the opportunity to explain a situation before decisions would be made," the Chief Security Officer said.*
>
> *"Throughout the communications, we really stressed the confidentiality aspect," he said. "These results weren't going to be shared with managers and the SVP of HR and I were the only two looking at these records—unless we needed more information. I think that really eased a lot of people's fears. This was between us and the employee, and issues were resolved, they were done."*

Phase III: Beyond the Initial Screen

Once the initial rescreen is conducted, the company decided to commence a "maintenance plan," whereby employees will be rescreened every two years, coinciding with their anniversary date.

Using an automated rescreen product with First Advantage, the company can be reminded when employee background screens are almost due, and can help automate the reorder process.

Fortunately, future screening processes will require less education and less communication—since employees have already been through the process once. Plus, the individual's identity information has already been verified, so the process actually gets easier with time.

If companies use an Evergreen Consent, which is available in many states, the process gets even easier—as the company has permission to conduct background checks throughout the course of an individual's employment.

> *"We could have just checked all our employees once and been done, but people live their lives and things happen to them every day," said the Chief Security Officer. "We wanted to provide assurances to our customers that we weren't just going to do this once, but that we would do it regularly.*
>
> *At the end of the day, it's good for our customers, good for our employees and helps solidify our reputation as an industry-leading provider."*

In Summary: Strategies for Employee Screening

- Use a core design team to establish the program design
- Get executive management acknowledgement and support early on
- Run pilot tests prior to full implementation
- Create an effective implementation team
- Limit data access to a very small group
- Communicate, communicate, communicate
- Educate employees via town hall meetings right before they begin the process
- Use a cross-functional implementation team

First Advantage
A Symphony Technology Group Company

We can help. For more information, contact First Advantage today:

Call: US +1-844-717-0510
Email: solutions@fadv.com
Visit: fadv.com

fadv.com