

An Acxiom White Paper

No News Isn't Always Good News:
Get the facts on vendor credentialing to protect your
employees, your customers and your company



Background checks are common practice when hiring new employees. But how about the people who interact with — or even represent — your company as vendors? Often, these individuals and businesses have access to your company information, assets and services, as well as having contact with your employees and customers. It's your responsibility to make sure that the vendors you choose to do business with have a history of operating with integrity. But how do you get the whole story on vendors?

Let's begin by determining who exactly is a vendor. A vendor might be defined as someone who sells a product or service to your business. A contractor, on the other hand, is typically a person or company hired to complete a specific job. These terms are sometimes used interchangeably, but any person — vendor, contractor or other external party — who has some level of access to your company assets is a candidate for credentialing.

While there is no standard definition of vendor screening or vendor credentialing, the screening process typically indicates a topical search that might include a criminal background check. The more in-depth vendor credentialing process delves deeper and can include a host of other searches, such as tax lien information, a fictitious business name check, insurance verification and a sexual offender registry check.

Third-party providers can deliver these and other vendor credentialing services that help identify the vendors you want to work with and — more importantly — the ones you don't. They can also help you navigate the complex and constantly changing world of privacy laws, keeping your company informed and operating within compliance.

Finally, and perhaps most crucially, third-party service providers can help you determine what exactly constitutes a sufficient background check, so you can cultivate an environment of security and confidence for your company, your employees and your customers.

Who needs to be checked?

Any individual or group entering your business or interacting with your staff or customers has the ability to make a positive or negative impact on your operations. With diligence and a little foresight, you and your vendors can enjoy a mutually beneficial relationship.

So, do all vendors warrant vendor screening or credentialing? In a word, yes. Any person or company able to gain direct contact with employees, customers, confidential data, financial files or proprietary company strategies should be scrutinized.

Ideally, all vendors should be held to the same level of screening as your regular employees. Why? If you are ever involved in an investigation or other legal matter due to the actions of one of your vendors, it is difficult to justify a lack of diligence in this area. Consistent screening across the board removes some element of vulnerability on your part, while eliminating any potential accusations of lax business practices or favoritism when it comes to vendor relationships.

If you think about it, there are a surprising number of outside individuals who have some level of access to your company assets, employees and customers. Beyond the obvious business vendors, you may also allow electricians, plumbers, repair persons, solicitors, consultants and many others to gain access to your facility. The majority of these individuals are honest people who perform their duties with integrity and excellence.

“The number-one important thing you can do is to understand what it is you’re outsourcing. And that sounds kind of simple, right? It’s like, well, I’m outsourcing my call center; I’m outsourcing the management of my security. But it goes much deeper than that. It’s actually understanding what’s implicated in the outsourcing structure from a risk management perspective. So if you’re outsourcing data, let’s say it is a call center, well, does that have insurance patient data, personal health data in there? Is it some other personally identifiable information that needs to be protected? You’re not just outsourcing a call center, it’s the data and the controls around that data that you’re also outsourcing.”

— Diana Kelley, Burton Group Analyst, in an interview titled “Security Secrets of Outsourcing,”
April 18, 2007, CIO.com

But not everyone operates with honesty and integrity. In today's fast-paced business environment, would-be criminals are as insidious as ever. It only takes a single opportune moment for one to wreak havoc in your business.

Vendor access opens the door to negative customer interactions, theft of company and employee property, theft of company, employee and customer data, and even physical violence against employees and customers. It's a frightening list, and it is up to the company — you — to do your best to prevent the possibilities from becoming realities.

According to Burton Group analyst Diana Kelley, companies should know their vendors and be familiar with their vendors' security processes. For example, Kelley points out that if a vendor is to have access to sensitive information, you need to know if that vendor performs internal criminal checks to identify any personnel who have been jailed for stealing data or selling credit card information.

SECURITY AND PRIVACY DRIVE CONSUMER PURCHASING DECISIONS

- **85% of Americans are worried about becoming victims of identity theft.**
- **64% of consumers say they had decided not to buy a company's product or service because they did not know how the company would use their personal information.**
- **58% of consumers say if they were confident a business followed their declared security and privacy policies, they would recommend that business to family and friends.**

— Source: Privacy & American Business, taken from Better Business Bureau "Security & Privacy — Made Simpler™"

"So you're outsourcing a lot of things," Kelley notes, "your reputation, the protection of the data, the risks associated with it, the regulatory compliance requirements around the data or even the business processes that are involved."

— Diana Kelley, Burton Group Analyst, in an interview titled "Security Secrets of Outsourcing," April 18, 2007, CIO.com

For the most part, vendor screening standards are still in development. For example, the healthcare, education and volunteer industries are experiencing increasing pressure and legislation to conduct due diligence in this area. But what constitutes “due diligence?” Reaching industry-accepted definitions and guidelines takes time, debate and practical application.

Any business or organization serving particularly vulnerable populations, such as children, the sick or the elderly, is at the forefront of this movement. However, vendor security issues also have a major impact on corporate businesses, and a lack of adequate screening can have devastating consequences.

Obviously, anyone having direct contact with compromised persons such as those listed above should be very thoroughly screened. Anyone having access to proprietary or confidential consumer or business information, such as Social Security numbers, credit information, other personal consumer data and corporate secrets, should also be closely scrutinized.

The debate, and confusion, arises when considering other types of individuals and groups, such as plumbers or electricians — people who have access to the grounds and employees or customers, but perhaps not direct access to computer data. Is it enough in these cases, particularly “emergency” situations like a burst pipe, to rely upon basic knowledge that the plumbing company you called for help screens its own employees?

It all comes down to a matter of risk, and the extent to which you can limit that risk. Unfortunately, many companies do not consider or concern themselves with risks from potentially dishonest vendors until a security breach has occurred. And then, of course, it is too late.

What is a background check?

As mentioned earlier, vendor screening is essentially a quick look to check for overt, red-flag problems. Since there are no hard and fast definitions of screening or credentialing, the extent of a background check can vary widely. One company might routinely contact references and conduct a criminal background check, while another might be satisfied with a quick Google search of public records. After all, increasing access to and reliance on the internet makes “do-it-yourself” online checking easier than ever, giving many business owners a dangerous and false sense of security.

Many risks aren’t easily discovered, and require a more thorough search than the average online user is capable of conducting. In fact, a dishonest vendor or one with criminal intent will oftentimes go to great lengths to deceive you. Vendor credentialing tools cast a much wider net than those available to most business owners, and provide a greater chance of unearthing the information that can ultimately protect you, your business and your employees.

Vendor screening versus vendor credentialing

Vendor Screening might include:

- A proprietary service, such as TRUSST®
- National criminal record check

Vendor credentialing might include:

- An extended, proprietary service, such as TRUSST + alias
- National criminal record check
- UCC filings
- Tax liens
- National corporation check
- Insurance verification
- Sexual offender registry check
- Secretary of state check
- Fictitious business name check
- Federal and state bankruptcy checks

How do I do it?

When it comes to maintaining security within your company, consistency is key. What good is it to develop good security practices if they are only being followed half the time? You must develop documented protocols and be committed to ongoing compliance training. Periodic internal audits, or “check ups,” should be used to identify vulnerabilities, and to ensure that all employees are following procedures.

A diligent screening partner can help you establish a consistent, effective plan to accomplish your security goals. In addition, a good partner will help you stay current on all applicable privacy legislation and industry-specific security issues to help you avoid potential problems and get the most out of your security protocols.

An ounce of prevention . . .

Establish good security and privacy practices now. The alternative is decidedly distasteful. If you have a data breach resulting from weak security practices, you and your business can face lawsuits from federal or state agencies or your customers.

— Better Business Bureau “Security & Privacy — Made Simpler™”

Where do I begin?

If vendor security is not a priority in your business, it's time to get caught up to speed. To get started, consider the following steps to increase security within your company:

- **Make a list of current vendors and others with access to sensitive material.** Are your relationships with these vendors in good standing? Is more access provided than what is actually needed for the vendor to provide service? Are there any vendors on the list who no longer have a relationship with your company, but could still gain access to sensitive information?
- **Compile existing security rules and search results.** Are all internal security measures being followed and enforced? Businesses can become lax in their own housekeeping, making themselves an easy target for dishonest individuals.
- **Determine who has access, and whether that access is appropriate.** Make a list of every person with keys or with computer access. Is this access necessary? Are there any missing keys? As your list of employees grows, it can be difficult to keep track of how many sets of keys are out there and who has them. Find out.
- **Interview all current vendors to learn whether they screen their own employees, and what security processes they have in place.** Make security a team effort. After all, a reputable vendor will support your efforts. A secure environment benefits everyone, including your vendor.

There are a number of commonsense, internal steps to take to increase security within your business, such as maintaining control over computer access and being aware of what individuals are entering and exiting your facility. With so much emphasis on protecting electronic data and computer access, businesses can sometimes overlook the physical security measures that should be taken into account.

Companies should use required employee badges, required escorts for visitors, sign-in and sign-out logs and security cameras. If possible, all doors into office space should be locked from the lobby. Companies should also provide employee education surrounding how to report seemingly "out of place" visitors, and training on how to respond to a variety of security breach scenarios.

In an interview about outsourcing security, Burton Group's Diana Kelley takes internal diligence one step further, stating, "You also need to specifically assign somebody within your organization to be the liaison with the vendor, to be the point person, whether it's the accountability person or the one that's checking the audit logs, or just talking to the outsourcer periodically to make sure that things are okay."

— Diana Kelley, Burton Group Analyst, in an interview titled "Security Secrets of Outsourcing,"
April 18, 2007, CIO.com

Better Business Bureau

Basic self-defense for your business

“Personal information” is information that allows you to identify an individual customer or employee. This might include such things as the individual’s name, address, age, gender, identification numbers, income, employment, assets, liabilities, source of funds, payment records, personal references and health records.

If your business maintains people’s personal information, you must protect that information from theft or misuse. Here are some basic rules:

If you don’t need it, don’t collect it. This seems obvious, but many businesses collect more information than they need. Here’s an example: Maybe your store wants to start e-mailing a newsletter to customers who have asked to receive it. So, you need each customer’s e-mail address. But someone suggests that — since customers are filling out a form anyway — maybe you should get their name, address and phone number as well. Then someone else suggests that getting customers’ dates of birth would allow you to e-mail a birthday card. So, instead of simply storing the information you currently need (the e-mail address), you end up storing a lot more. The more you have, the more tempting it becomes to a thief and the more damaging it is to your customers if the information is stolen.

If you need it once, don’t save it longer. Companies sometimes collect information that’s necessary to complete a single transaction, then compulsively file that information away (either in a paper file or in a computer file). For example, what happens to job applications for people you don’t hire? These contain all sorts of personal information, including the all-important Social Security number. Again, if you aren’t required by law to keep the information, and you seldom, if ever, use it, then get rid of it. If you don’t keep it, it can’t be stolen.

If you’ve got it, but you don’t need to save it, dispose of it carefully. As we’ve pointed out in our general advice to consumers, a good deal of identity theft happens in the trash barrel or dumpster. Even the smallest business can afford an inexpensive paper shredder. Make sure you use yours to destroy customer or employee records.

If you have to keep it, think security. First, make sure those paper records that contain personal information are kept under lock and key when they aren’t in use. Make sure computer terminals are password protected. Limit the eyeballs that have access to these records — only those who have an absolute need-to-know should have access to personal information. Don’t allow customers or others to wander around the private areas of your business.

Don't broadcast personal information. How often have you stood in line at an office or store behind someone who was being asked to give his/her Social Security number or telephone number or birth date? How many times have you watched a company's employee pull up personal information on a computer screen that was visible to other customers? Or seen personal information on a file that was left open on a desk or counter? Instruct your employees to be sensitive to these issues. Turn computer screens so they can't be viewed by anyone other than the operator. Instruct employees who need to have personal information to have customers jot that information down, not repeat it out loud where it can be overheard by others. Don't put personal information like account numbers in billings or letters where that information is visible through windows in the envelope.

Don't use Social Security numbers as account numbers. While not common, this practice is just downright dangerous — to you and your customers.

Don't give out employee or customer information to anyone whose identity can't be positively confirmed. Information thieves and stalkers tell authorities over and over how easily they were able to obtain all sorts of valuable information simply by calling small business owners or personnel departments and asking. Posing as government agencies or credit grantors or health insurance providers, these thieves have found that a well-crafted, believable story can often get past the best locking file cabinets or password-protected computers. Your organization should have very strict policies on when and how employee or customer information is shared.

Locks and alarms are a real deterrent. If you've done everything we've suggested, your records — and your customers — will be more secure during business hours. Make sure you're at least as secure when your business is closed. Make sure all vital records and offices are locked during non-business hours. Exterior doors should have deadbolt locks. Hinges on exterior doors should be secured to prevent removal. Exposed windows should be protected with bars, screens or shatter-proof glass. The business' exterior should be adequately lighted from dark to dawn. Naturally, the business should be protected by an alarm system, preferably one that is monitored by the security company.

— Better Business Bureau, "Information for Businesses — In the Real World"

Why use an outside service provider?

Beyond internal security measures, every business — particularly those with multiple locations — can benefit from an external security service provider. It takes a security services professional to know what searches need to be conducted, and how to obtain the information that helps you make an informed vendor decision.

Once you contact an external provider, expect to be asked questions about your current processes, your screening budget, those individuals at your company authorized to request checks and receive results, your technological/communication method preferences and more.

External service providers can search available records in order to verify a vendor Social Security number, detect fraudulent numbers and flag numbers that have not been issued by the Social Security Administration or have been filed with death claims. Alias and maiden names can be discovered through utilization of the Social Security Number Trace.

Competent screening vendors can also assist in conveniently ensuring consistency among decentralized offices or branches through management reports, customized exception reporting and legislative updates that a company may not have the resources or expertise to stay abreast of on its own.

If using a reputable screening company, employers will likely be asked to execute agreements that may not necessarily be binding in terms of time frame, but that indicate an understanding and acceptance of his/her obligations as an employer requesting and using personal data.

Proprietary solutions

Proprietary services within the industry can provide additional benefits, such as one that targets counties in which applicants have resided, but have not disclosed, to uncover possible criminal histories. These types of in-depth services increase “hit” or record ratios, or the overall percentage of applicants found to have criminal histories.

Vendor credentialing might include identification and Social Security number verification, national criminal record check and UCC filings. Additional services available within the industry include:

- Motor vehicle record report
- Employment verifications
- Professional license verification
- Education verification

Custom services are also available, designed specifically to meet a client's particular security needs.

Utilizing all available services lessens the possibility of allowing a criminal into your corporate family. This is why it is so important for companies to understand the internal screening processes used by their vendors. Security screening can prevent a number of disastrous scenarios, and each layer of security — your company, your vendor, your proprietary services partner — provides additional protection.

“Your vendor could be very, very adept at what they’re doing. They could actually have better processes and better security than you do, but you can’t just trust that blindly. You still have to get a handle on the level of risk management you require, and then make sure that that outsourcer’s up to it.”

— Diana Kelley, Burton Group Analyst, in an interview titled “Security Secrets of Outsourcing,” April 18, 2007, CIO.com

Look for a partner who takes a comprehensive approach to vendor credentialing, with ongoing services and industry alerts for their clients. Security updates, industry concerns and new legislation can be communicated to clients via phone, fax blast, monthly electronic news, quarterly news and field training, to ensure timely updates and business compliance. Proactive methods help clients stay abreast of the changing vendor security landscape, and provide a valuable and trusted resource. Benefits should include:

- **Speed and accuracy.** Background screening reports should be created from real-time research of public records and other sources (unlike some services that create such reports from rapidly aging and often incomplete databases). To avoid inaccuracies, look for a vendor who does not involve a third party.
- **Risk mitigation.** Assists in the prevention of potentially dangerous or untrustworthy people from joining the ranks of a company, thereby limiting legal exposure and the risk of injuries, violence, theft, and property damage.
- **Privacy and legal compliance.** Engaging outside experts helps employers in their efforts to ensure that background checks are conducted in a legal, ethical and consistent manner that benefits the company while protecting the privacy of individuals.

Service providers are not created equal. Some providers return more criminal hits on applicants than other providers, depending on the level of their criminal and address history searches, as well as the thoroughness of the screening company's data scrubbing and information re-verification processes. It is in your best interest to be selective when it comes to choosing the right provider. After all, discovering undesirable information up front allows you to avoid — rather than deal with — potential security risks posed by vendors.

Among the most important benefits of partnering with a vendor security provider is the extraordinary legal insulation that is available to your company. A good provider brings deep experience and consistency in research and reporting systems, which translates to a detailed, proactive understanding of the legal obstacles your business might face.

A great service provider should also provide outstanding compliance support and training. In fact, this issue is so important that a diligent provider will require that all team members complete a privacy compliance training course. Look for these and other high standards when choosing a provider, to receive the best service and support possible.

Summary and conclusion

Vendor credentialing is a complex, but essential, process. All businesses can benefit from the help of an outside service provider to assist with security services and compliance, particularly those businesses with multiple locations.

Service providers are not created equal. Therefore, when choosing a service provider, businesses should look for one that has high internal standards, a history of exceptional service and a suite of in-person, real-time search options. To avoid inaccuracies, these searches should not include standard third-party involvement.

Ultimately, you are looking to partner with a team of highly trained professionals using the most sophisticated technology to provide you with accurate information about potential vendors and subcontractors – quickly and cost effectively. Take advantage of proprietary solutions within the industry, such as a supplemental, comprehensive database for added results and expanded search options.

Most vendors are honest individuals and businesses looking to establish a mutually beneficial relationship. But there are exceptions, and those potentially dangerous vendors will only tell you what they want you to hear. It's up to you to uncover the rest.

See how Acxiom can work for you.

For more information, visit our website at

www.acxiom.com/backgroundscreening or call:

1.800.853.3228

