

## Do You Know Who You're Hiring?

Christopher Marquet

---

He was considered a dream candidate for the job.

A former high school football coach from Utah, Duane C. Johnson seemed eminently qualified to teach in Nevada. He produced excellent letters of recommendation, Utah officials had nothing but good things to say about him when contacted, and he was enthusiastic about working with troubled youngsters.

So, when a job opened at a local shelter for neglected children, school administrators in Las Vegas hired him immediately. Qualified teachers were scarce, and they believed they had found a perfect fit.

But they were wrong. Within a year, a 13-year-old girl accused Johnson of sexual misconduct, and only then did the people who hired him realize they had made a grievous error.

In the pre-employment interview, Johnson had acknowledged that his Utah teaching license had been revoked—but claimed the action was unjustified and he was challenging it. They had accepted his explanation, ignoring the fact that revocation of a teaching license was a red flag signaling the need for further investigation.

An effective background check would have revealed that he had lost his Utah job after being accused of impregnating a student. All Nevada officials needed to do was dig a little because the incident had been reported in the local news media. Failing to do that and to confirm the validity of Johnson's account, they had hired an accused child molester to work with very vulnerable children. For their narrow reasons—Nevada needed a teacher and Utah wanted to get rid of one without facing the difficulties of criminal prosecution or protracted disciplinary action—officials of both states had participated in “passing the trash.”

HR executives know that such situations are neither unusual nor limited to the education sector. “HR managers are often so in need of warm bodies, they just don't want anything to be wrong with a candidate who looks good,” says Nancy Lovallo, a former Director of Human Resources at a large teaching hospital in the New York metropolitan area. But relying on looks, taking resumes at face value and failing to conduct appropriate background checks can lead to big trouble and costly mistakes.

Recently, falsified resumes submitted by high-powered executives have damaged the reputation and financial standing of some well-known, publicly traded companies and at least one prestigious university. Notre Dame's new football coach was forced to resign just five days after being hired because his resume contained falsehoods about his experience and credentials. The hiring fiasco hurt the school's credibility and prompted hard questions from alumni, who provide a high level of financial support.

More examples: On the day MCG Capital Corp. disclosed that its founder did not graduate from Syracuse University, company stock fell 37%. Similarly, the stock of Veritas Software Corp. plunged 19% the day it fired its CFO, who lied about having

earned an MBA from Stanford.

Such oversights—and their fallout—are not limited to high-profile organizations. According to the Association of Certified Fraud Examiners (ACFE), most employee screening mistakes occur in organizations with fewer than 100 employees. What's more, while the Society for Human Resources Management reports that 70% of organizations and corporations claim they conduct "background checks" on new hires, evidence suggests these checks may not be effective. Overall, businesses lose about \$400 billion annually to employee fraud, and the average company loses 6% of its annual revenue to employee theft, according to the ACFE. Additionally, Department of Justice statistics indicate that workplace violence, threats and abuse continue to be significant problems, with 25% of workers reporting that they are attacked, harassed or threatened in the workplace each year.

"You must know who you're hiring—especially since the September 11th terrorist attacks," says Paul Viollis, Senior Managing Director and Security Services Practice Leader at Citigate Global Intelligence & Security, a New York-based firm that provides businesses with intelligence and investigative services, including those focusing on employee integrity issues.

"Every employer is obligated to provide a safe environment for employees and other individuals they deal with," he adds. "They must validate the integrity of their employees. If a job applicant or candidate lies on an application or during an interview, chances are he or she will lie on the job."

Skilled and knowledgeable HR executives, not seduced by claims to fancy degrees, reports of significant accomplishments and a pleasant demeanor, believe that effective Employee Integrity Programs begin with meticulous and thorough screenings. "Solid investigative methodology involves multiple attempts to verify the information provided by the applicant," Viollis explains. "But, the depth of a background check should be correlated to the responsibilities and risk associated with the position being filled," he cautions.

Generally a strong background screening procedure is documented in writing and includes the following:

- Compliance with the Fair Credit Reporting Act, which mandates that applicants sign a release consenting to a background check prior to employment and agreeing to ongoing background checks during the course of employment.
- Confirmation of employment history, with special attention to gaps in time between jobs, job titles, declining salary history and reasons for leaving a former job.
- Verification of education and technical credentials, including obtaining transcripts of degrees, professional licenses and certificates documenting credentials.
- Skillful candidate interviewing to determine more than what the applicant is revealing. Confusion about self-reported history is a warning sign.
- Interviews with personal and professional references and non-references,

including supervisors, co-workers and neighbors.

- In-depth scrutiny of public records, including civil litigation histories, criminal records, motor vehicle and credit reports and notices of bankruptcy, judgments or liens.
- Corroboration of military history.
- Examination of media references, websites and Internet discussion sites.
- Analysis of handwriting and psychological testing.
- Testing for substance abuse.

Such extensive screening can be expensive. But in today's less secure business climate, with its highly mobile society and transient working population, failure to dig deeper and detect unsavory backgrounds can result in irreparable damage that can be far more costly than employee misconduct, fraud, theft and increased legal and insurance costs.

"Problem employees can cause the fabric of a firm's well-functioning team to unravel," says Lovallo. "This can produce major losses resulting from the crippling effects of low morale, lost productivity, reduced competitive advantage, damage to corporate reputation, expensive litigation and even physical injury and death."

Many employment specialists believe that a key reason to conduct accurate and comprehensive employee background checks is to avoid a "negligent hiring" lawsuit, which can result in substantial financial penalties, including actual and punitive damages.

According to the Doctrine of Negligent Hiring, employers are accountable for placing individuals in specific positions. What's more, the doctrine stipulates that employers can be held liable for employees' actions—including some acts outside the scope of employment—if it can be shown that they failed to make "reasonable" inquiries into an employee's background and suitability for the position.

Although not a law, the doctrine is upheld in more than 30 states. Most negligent hiring lawsuits maintain that the employer failed to conduct a "reasonable" investigation into the job candidate's background, which could have disclosed the possible risk of harm or injury to coworkers or third parties. The bottom line is simple: Courts are making employers responsible for what they know or should have known had a "reasonable" background check been completed.

What is "reasonable"? " 'Reasonable' is defined by case law and experts, and obviously depends on the nature of the position being filled," explains Viollis. "Some states place different restrictions on the type of information available to companies, and it's vital that employers present potential hires with documentation about background screening before beginning the screening process."

Since September 11th, security experts say, a greater level of care in vetting potential employees is essential. That's why companies are being urged to upgrade the quality of their employee background checks.

But getting at the truth—as seen in the case of Duane Johnson and the Nevada school

system—often takes willingness by HR executives to expend time, effort and money. Extensive background checking can be costly, but Viollis believes that in these times “we can’t put dollars over safety,” and using budgetary restrictions as an excuse for conducting superficial investigations no longer is valid.

“If my client sues your company for injuries sustained by one of your employees, and you claim you didn’t have enough money to conduct an appropriate background check, I can subpoena your budget,” he explains. “If I find that you had the money, but simply didn’t allocate it for employee screening, I’m going to have a hard time agreeing that you were unable to conduct a proper investigation.”

He adds: “In today’s world, at the end of the day, employers must accept responsibility for the integrity of their employees. Doing nothing is no longer reasonable.”

### **SIDEBAR – for Effective Employee Screening**

#### **Important Behavioral Warning Signs**

While profiling can be controversial, it is often helpful to keep the following in mind when investigating an employee’s behavior.

#### **Profile of a Typical White-Collar Criminal\***

- Middle aged (sex/race not a factor)
- Longer-term employee
- Holds position of trust
- Takes little vacation
- Likeable, helpful, knowledgeable
- Living beyond means/financial difficulties
- Substance abuse problems
- Gambling problem
- Marital/relationship problems
- Emotionally unstable

**\* Source: Citigate Global Intelligence & Security**

#### **Profile of a Potential Attacker\*\***

- Male – 30-50 years old
- Usually quiet and distant from coworkers
- Loner, little family, church or community support/involvement
- May display erratic/unusual behavior/habits

- Chronically disgruntled
- Substance abuser and/or mental health problems
- Does not hold consistent employment
- Admits to fascination with weapons
- Does not handle criticism well
- May have conflict with management and/or personal issues with others

**\*\* Source: Citigate Global Intelligence & Security**

## Author



**Christopher Marquet**

[chris.marquet@citigategis.com](mailto:chris.marquet@citigategis.com)  
[www.citigategis.com](http://www.citigategis.com)

Christopher T. Marquet is Executive Managing Director and Principal of Citigate Global Intelligence & Security (CGIS), based in Boston. Mr. Marquet is a member of the CGIS Executive Committee and a senior practitioner in all three core capabilities of the firm—Business Intelligence, Business Investigations and Business Controls & Security. He is also responsible for oversight of the Security Services practice and overall business development for CGIS worldwide. Mr. Marquet has nearly 20 years of professional experience in the investigative, intelligence and security industry.

Prior to joining CGIS, Mr. Marquet was Senior Managing Director and head of Kroll Inc.'s operations in the New England region. Mr. Marquet also served as Senior Managing Director and head of worldwide business development for Kroll, based in its New York City headquarters. In that capacity, Mr. Marquet was responsible for all marketing, sales and public relations activities worldwide.

Mr. Marquet also served as Managing Director and head of Kroll's online global risk assessment division and President of Kroll Travel Security Services, Inc. Mr. Marquet helped create and launch innovative online and print publications covering travel security issues. Named the youngest Managing Director in that firm's history in 1993, Mr. Marquet was a senior member of the international division responsible for managing key strategic relationships. During this period, Mr. Marquet was intimately involved in the firm's highly publicized engagements on behalf of the Russian and Brazilian governments, as well as numerous other sensitive international investigations.

During his lengthy career, Mr. Marquet has been involved in thousands of business intelligence, investigative, litigation support and security consulting projects around the world. These matters have been diverse, but include many business, competitive intelligence and due diligence projects, general litigation support investigations, intellectual property theft investigations, asset searches, hostile takeovers and proxy battles, internal investigations and employee misconduct inquiries, fraud investigations, workplace violence threats, corporate security assignments, executive protection, crisis management and insurance dispute investigations. Mr. Marquet has lectured extensively and is the author of articles relating to due diligence, investigations, fraud, employee integrity, workplace violence, kidnapping, terrorism, crisis management and travel security.

Mr. Marquet is a member of the Massachusetts Bar Association, the American Society of Industrial Security, the Association for Corporate Growth and the Risk & Insurance Management Society. He received an A.B. degree from Dartmouth College in 1983, with a triple major in physics, economics and philosophy.

## About Citigate Global Intelligence & Security

Citigate Global Intelligence & Security, a wholly owned subsidiary of Incepta Group, plc, is an international business intelligence, corporate investigations and business controls firm focused on helping clients meet increased intelligence, compliance and security needs. CGIS offers clients seamless access to leading practitioners in the fields of business investigations, due diligence, hostile takeovers, business and

competitor intelligence, forensic accounting, business controls, commercial disputes and corporate security. CGIS is headquartered in New York with offices in Los Angeles, Boston, Miami, Dallas, Chicago, Atlanta, Washington, D.C.; and international offices in Geneva, Switzerland; Quito, Ecuador; and Tokyo, Japan.