

The first firewall: Background checks as India Inc.'s frontline defense



Username



Password

Forgot your password?

☐ Remember me

Login



The better the question.
The better the answer.
The better the world works.



Shape the future
with confidence

Contents

Foreword	03
Executive summary	04
Healthcare	06
Financial Services	10
IT/ITeS	12

Foreword

As the world continues to adopt technology in every aspect of our lives, the risks that come with it are evolving at an equally rapid pace. CHROs and HR professionals are now facing an emerging risk landscape that includes challenges such as fraudulent employment records, moonlighting, falsified credentials, the use of deepfakes in online interviews, and dual employment. In this evolving environment, it is crucial to adopt a strategic approach to risk management, powered by technology to detect and address emerging risks by prioritizing employment background checks, and developing comprehensive policies.

Over the years, traditional background verification methods have proved to be inadequate, time consuming, and prone to human errors. Advanced background verification systems are increasingly becoming the future of HR management. By leveraging automation and sophisticated data analytics, these systems provide a more comprehensive and efficient approach to verifying candidate credentials. This strategic shift not only enhances the accuracy and reliability of background checks but also supports HR professionals in cutting down on dependencies on third parties and reducing the TAT, resulting in faster onboarding and deployment on billable projects.

Employee onboarding is the critical first step in the employee lifecycle, setting the tone for their engagement and establishing a foundation of trust that evolves throughout their tenure with the company. However, this critical phase also introduces potential risks, as employment fraud poses a serious threat to organizational integrity, exposing the company to a host of threats that can have financial, operational, and reputational ramifications. Every sector, from financial services to healthcare and information technology (IT/ITes) to construction—is currently grappling with this challenge.

The prevalence of counterfeit employment certificates has risen to concerning levels and is currently posing the biggest risk to most sectors. These falsified documents are not only inexpensive and easily procured, but they can also be generated within a few hours—which makes it extremely lucrative to those with insufficient experience. As businesses navigate the complexities of the modern workforce, embracing digital background checks is not just an option—it is a necessity. AI-driven screening and document authentication-based verification are transforming background verification into a seamless, efficient, and more reliable process.

Drawing on our expansive experience in extensive background verification engagements across sectors, we have observed critical issues that, if left unaddressed, could pose significant threats to organizations. This is especially true in terms of understanding the need to opt for sector-specific background checks. This can help expand the scope of the process from a mere box-ticking exercise to a value addition. With the government placing utmost emphasis on compliance, adherence to regulatory norms is mandatory, but implementing proactive measures in place can make it a business differentiator. Harnessing the might of technology-led background verification solutions can not only help companies reduce turnaround time considerably, but also present an insightful and accurate report for better decision-making.

This report highlights sector-specific trends in employment fraud and underscores the urgent need for preventive measures. We hope this report helps you glean the importance of integrating automated background checks as a fundamental part of the hiring process. By doing so, businesses can significantly reduce the risk of employment fraud, protect their assets, and ensure that their workforce comprises trusted, qualified professionals.




Arpinder Singh

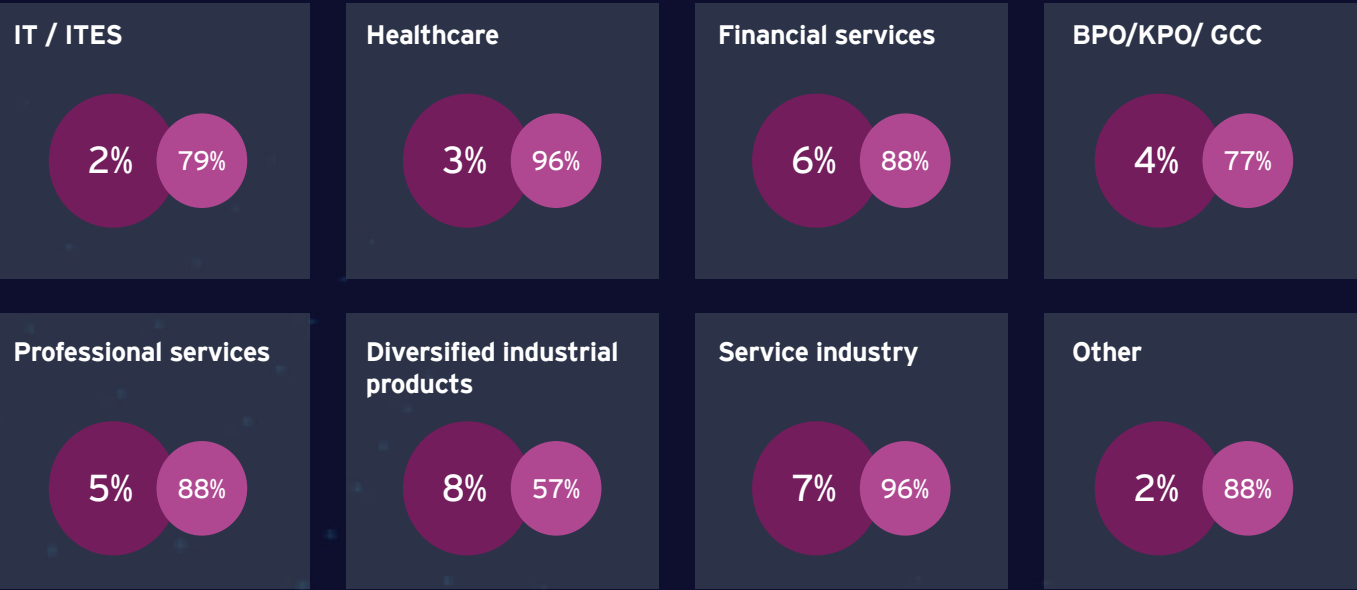
Global Markets and India Leader,
EY Forensic & Integrity Services

Executive summary

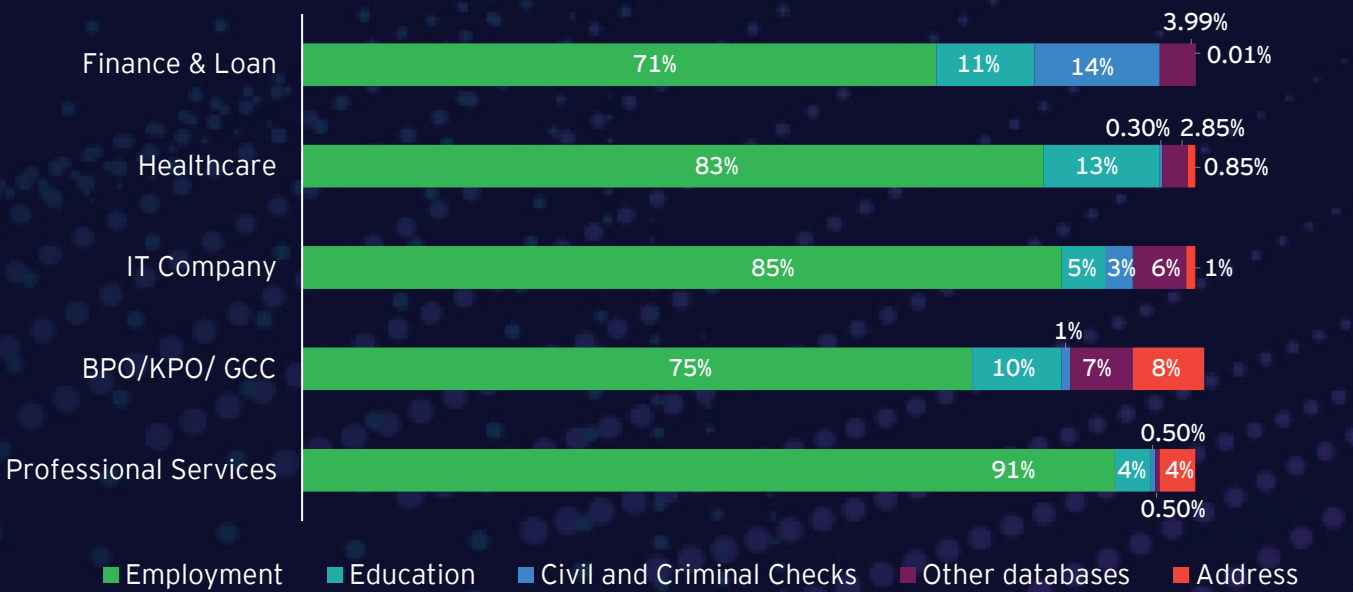
In this document, we have highlighted the results obtained from background verification in different sectors. It also offers insight into the major reasons for discrepancies and explains how each sector faces different challenges during candidate onboarding.

We have conducted over a **>1 million** checks across different sectors, and the discrepancies observed in each have been captured in this report.

 % of share in the reports  Experienced candidate causing red reports

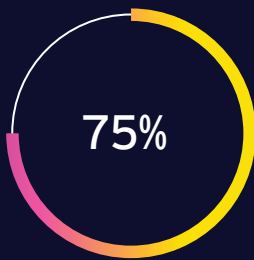


The top reasons for discrepancies across the five major sectors - IT/ ITeS, financial services, healthcare, BPO/ KPO/ GCC and professional services- are classified below:

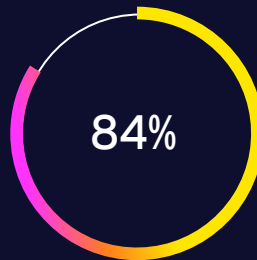


Major reasons for discrepancies:

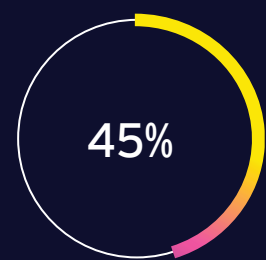
Employment



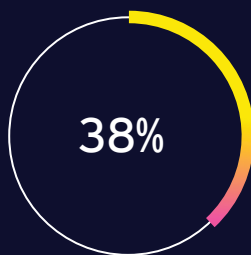
of the candidates had submitted fake employment documents in Healthcare sector



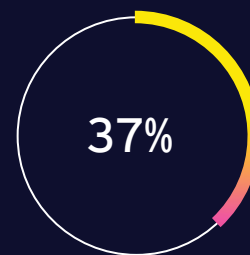
of candidates had overstated their experience in Financial Services sector



profiles of the ones marked as discrepant were found to be moonlighting in IT sector



of the candidates did not provide mandatory documents, such as experience letter or service letter, nor did they provide UAN linked consent in the BPO/ KPO/ GCC sectors



of the candidates had additional employments, which was noted as per UAN records. However, the same was not disclosed in the Professional Services sectors

Education

50%

candidates had submitted fake education certificates in Financial Services sector

84%

candidates had obtained certification from an institute which was categorized as "Not Accredited/Approved/Fake" by governing bodies in the Healthcare sector

6%

candidates had degrees from universities which were part of the client's "no hire" list

54%

candidates did not provide education certificates for verification in the BPO/ KPO/ GCC sectors

88%

candidates had submitted fake documents in the Professional Services sectors

IT/ ITeS, healthcare and financial services sectors have seen the largest number of recruitment and were among the first to implement structured and third-party validated background checks. Let us delve deeper into the detailed analysis of the three sectors that are at the forefront of our employee background check engagements.



Healthcare

The healthcare industry in India has been witnessing dynamic growth over the past decade to meet the needs of the country's population, increased health awareness, and the evolving economic landscape that encourages expansion. Health expenditure has increased from 1.4% of the GDP in 2017-18 to 1.9% of the GDP in 2023-24, as per the findings of the States Economic Survey 2023-24, conducted by the Ministry of Finance. The Union Health Ministry has increased the allocation for health care expenditure by 12.59% in the interim budget for FY 2024-25, suggesting many more government initiatives to further the healthcare industry.

Proactive regulatory reforms and supportive policies have helped define its growth trajectory to be in line with compliance requirements. The private sector, non-profits, healthcare start-ups, and international chains setting up shop in India have further augmented access to advanced medical services and fostered innovation in healthcare delivery. There is more focus than ever before to equip healthcare professionals with the latest technologies that can revolutionize patient management. This can be further seen with the increased investments in health care space from large private equities.

A leading destination for medical tourism, India attracts hordes of health travelers annually. However, hospitals must secure Joint Commission International (JCI) accreditation to qualify as a hospital registered with the medical tourism division.

To get accredited, it is imperative that healthcare professionals recruited by the hospital possess necessary qualifications to provide safe and efficacious care, and that it is thoroughly documented. The healthcare sector has been grappling with a talent shortage, and with the increase in demand for qualified professionals, fraudulent candidates are scheming unethical ways to get hired. There is a high turnover of almost 40% to 50% amongst junior staff and nurses. Considering the sensitive nature of the job, onboarding candidates with forged credentials can literally be a matter of life and death.

EY has been working closely with some of the largest healthcare companies in India, conducting background checks on four categories of healthcare employees.

Most large healthcare chains get the following checks on different categories of employment:

- **Doctors and nurses:** State registration, employment and CRC
- **Pharmacists:** Education, employment and CRC
- **Support staff and paramedics:** Education, employment, address and CRC
- **Corporate staff:** Education, employment, address, CRC and global database

While most large healthcare organizations do not opt to conduct criminal check or address verification, as part of their background verification process, there were instances where candidates had submitted fake addresses or had open cases against them, especially in medical negligence cases, thus increasing the exposure of the health care providers.

Here are some of the findings that will help understand the extent of the discrepancies in background checks that the sector is currently facing:

Of the candidates with discrepant profiles, 83% failed to comply with employment checks and 13% had education checks-related issues. Submission of fake documents by candidates has been the biggest red flag in this sector.



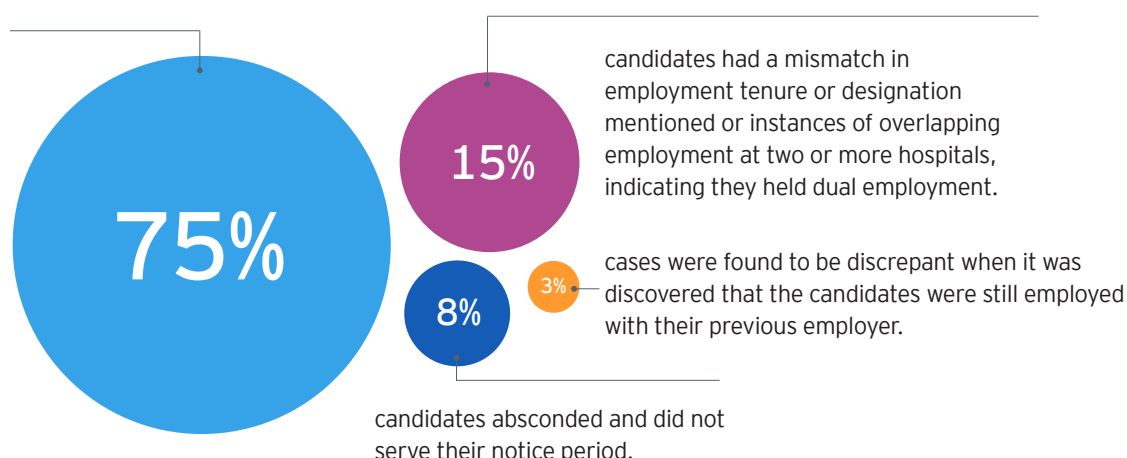
Ensuring that healthcare professionals hold valid licenses and certifications is crucial within the medical sector to confirm their qualifications and legitimacy to offer services in their specialty. This practice is key to maintaining high standards of patient care and minimizing the incidence of clinical mistakes.

Amit Rahane, Partner, EY Forensic & Integrity Services

Employment discrepancies

Of the **83%** discrepant employment checks:

Candidates had submitted fake documents, where during employment checks, it was confirmed that the candidate had never worked with a previous employer. It is pertinent to note that out of these 75% cases where fake documents were submitted by candidates, 30% fake experience letters mentioned employment with 10 largest healthcare facilities in India, making candidate profile appear stronger. In these instances, our document authenticator tool can find fraudulent or digitally manipulated documents.



Fake credentials

In December 2024, a fake medical certificate racket was caught in Gujarat, followed by another such incident in February 2025 in Hyderabad, where individuals were issuing certificates from recognized universities in exchange for hefty sums of money.

It did not come as a surprise then that **16%** of education checks conducted by us, as part of our engagements with our healthcare clients, proved to be discrepant.

84% candidates had obtained certification from an institute which was categorized as “not accredited/approved/ fake” by any governing body, thereby discrediting the quality of education. We have noted that in many instances, due to lack of talent, some large healthcare chain still go ahead and onboard candidates if all other checks are clear and only their certification is from an unaccredited institute.

Pending court cases

Criminal background verification is one of the most crucial checks that must be performed before onboarding a candidate, especially considering the highly sensitive nature of the sector. However, many large healthcare providers do not even conduct the CRC checks. We noted that 0.30% of the cases, where these checks were performed were flagged due to candidates' involvement in pending court cases or in criminal cases filed with the local police station.

In conclusion:

The obligation of the healthcare sector to protect lives underscores the importance of employing individuals who are not only qualified but also ethical and reliable. Hiring fraud can result in reputational damage, legal liabilities, and significant financial repercussions. Incidents involving impostor physicians, unqualified nursing staff, and negligent behavior often costing lives emphasize the need for thorough verification of healthcare professionals' backgrounds. Implementing exhaustive background checks can inspire patients' confidence and meet regulatory bodies and stakeholders' demands.





Financial Services



India's digital transformation story is one for the books and the impact of this change is most evident in the financial services sector that has been growing by leaps and bounds in the last five years. FinTech start-ups have been the catalysts for boosting this growth further through innovation. These mushrooming platforms proved to be complete gamechangers when it came to simplifying complex financial products for the larger market. There is also a proliferation of domestic and multinational banks, NBFCs, insurance companies, mutual funds, and capital markets thriving in India.

Many financial institutions are looking at the country to set up their GCCs, and several companies have already established one here, which is a very encouraging trend. The government has approved 100% FDI for insurance intermediaries and increased the FDI limit in the insurance sector. Credit, insurance and investment penetration are rising in rural areas, and HNWI participation is growing in the wealth management segment. Not only do these achievements reflect the growing strength of India's financial industry, but also denote its potential to become an attractive hub for investments.

With India slowly inching its way towards becoming a cashless economy and government's impetus towards it, digital transactions are becoming faster, safer, and more transparent. Budget 2025 underlines India's emphasis on strengthening the building blocks of the financial services sector by boosting consumption opportunities, increased housing demand, transforming rural credit access and supporting MSMEs. Adoption of AI and ML capabilities will provide fillip to digital infrastructure for sustained growth.

Given the sector's positive outlook, attracting talent is not a challenge for human resources function, but its lucrative prospects also necessitate tackling the menace of employment fraud. The Reserve Bank of India (RBI) has mandated that banks carry out thorough background screenings for individuals hired from other financial institutions and emphasized the responsibility of banks to verify that their recovery agencies refrain from hiring individuals with a criminal record.

The financial services industry generally conducts more thorough verifications compared to numerous other sectors, given that its workforce is frequently responsible for managing monetary assets and confidential client information. Checks into financial backgrounds might encompass an assortment of checks, such as verification of previous employment, educational credentials, and potentially criminal backgrounds. Automating background checks is one way of doing this.

In our work with financial services organizations across the country, EY has noted discrepancies in experience claims made by candidates, overstating of designation, and fake educational qualification certificates.

Of the 6% discrepant profiles, 71% had been flagged off during employment checks, 18% failed to clear civil and criminal checks, 11% had education qualification gaps, and the rest were found to be discrepant during credit score check.

Forged documents

5% of discrepant employment checks were due to candidates submitting doctored or completely forged documents to support their candidature.

The issue of forged documents plaguing HR departments of the financial services sector is a grave concern considering the hired professionals would be dealing with sensitive documents in their line of work. Of the forged documents submitted were proof of remuneration, reflecting inflated compensation instead of actual salary. There were also some candidates with records of parallel employment or those who had absconded from previous employment without completing their notice periods.



In the realm of financial services, a wealth of confidential data is at risk of falling into unauthorized hands. Attaining tranquillity is possible when you're assured of the integrity and commendable history of your employee. Furthermore, being informed of their previous missteps allows you to sidestep similar pitfalls. Consequently, numerous firms implement thorough background screenings of prospective hires prior to finalizing their employment decisions.

Amit Rahane, Partner, EY Forensic & Integrity Services

Misleading information

84% of discrepant employment checks were due to misleading information shared by candidates. These profiles* were flagged off due to mismatch in designations proclaimed by the applicants on their CVs or experience letters. In some instances, the period of employment submitted by the candidate did not tally with HR records.

Other information identified during verification

In few instances, during verification, the HR confirmed that the candidate had absconded the organization. Several instances were noted wherein the candidate was still employed with the organization. There were also some candidates with records of hidden employment which were identified during employment and other checks.

Education qualification gaps

Of the discrepant profiles who failed education qualification checks, 50% candidates had submitted fake education certificates where in the University through letter responded on the education details confirmed that candidate details were not found in university records. The balance 50% candidates were found to have submitted certificates from institutes categorized as "not accredited/approved" by governing bodies.

Involvement in criminal/civil cases

Reputational damage can cause financial services organizations to lose all their credibility, which is why it is imperative that the criminal backgrounds of all potential employees are thoroughly verified. There were a few instances where candidates were found to be involved in criminal/civil court cases, which were flagged off so organizations could make an informed choice.

In conclusion:

Background screenings allow companies to better protect client funds, verify the suitability of their staff for the positions, promote a positive workplace atmosphere, and act as an early warning sign. When it comes to financial services, it is crucial to recognize that performing criminal and financial background investigations can uncover previous offenses that could render an applicant ineligible for a certain job or signal caution to entities governed by local regulations. Moreover, elements like a recent bankruptcy, a record of financial fraud, or outstanding legal judgments may suggest a heightened risk of the individual engaging in fraudulent behavior.

IT/ITeS



India's IT sector has been undergoing significant transformations, especially since digitalization. The sector is rapidly evolving with traditional outsourcing, making way for advanced solutions. Emerging trends such as cloud-first strategies, AI integration, cybersecurity innovation, and blockchain technology are redefining the scope of the sector even as India continues to lead global outsourcing and digital transformation services.

The tech industry in India is anticipated to expand more rapidly in the current financial year, fueled by advancements in engineering research and development, along with an increase in the establishment of Global Capacity Centers (GCCs), which serve as cost-effective offshore bases. The demand for skilled talent in emerging technologies will grow, and India's IT firms will expand their global market share, especially in emerging markets. There has been a transformation in the pattern of revenue allocation, with Indian service providers and international conglomerates, encompassing GCCs, now equally sharing in the contribution to the industry's export earnings. According to NASSCOM, the sector is expected to add 126,000 jobs on a net basis, taking the total workforce to 5.8 million in fiscal year 2025.

With the growth potential in the industry, short fuse requests will increase, thus making the speed at which background verification is done of utmost importance. While the sector's progressive approach towards innovation is promising, it does have to tackle its share of frauds. Recently, there has been a spate of incidents where IT companies have come under the scanner for their treatment of its employees. Considering that their every move is being watched, it becomes imperative for IT organizations to be thorough in their hiring process. The hybrid workplace has highlighted the issue of dual employment rampant in this sector. Moonlighting employees not only threatens the integrity of an organization, but they also pose a serious challenge in terms of maintaining confidentiality.

Currently, major corporations are scrutinizing the work performed by applicants throughout the COVID period, regularly revising their "do not hire" lists to include certain companies and educational institutions. As a prudent practice, some large tech organizations also provide a list of all the companies from where they had hired their employees to cross-verify the existence and reputation of the company. This helps them to update their "do not hire" list. They are also enlisting the help of background check providers to station representatives within their offices to streamline the document collection process. To handle the substantial number of insufficiencies, organizations gather all necessary onboarding documents before extending job offers and also revise their lists of minimum requirements.

Tech companies are also enlisting the help of background check providers to station representatives within their offices to streamline the document collection process. To handle the substantial number of insufficiencies, organizations are gathering all necessary onboarding documents before extending job offers and are also revising their lists of minimum requirements.

Of all the discrepant profiles flagged off, 85% were due to employment checks, 6% failed other database checks, 5% were found to have discrepancies in their education claims, 3% had pending civil and criminal cases against them. The biggest issue faced in the industry included those of moonlighting either through additional employment or other business associated with them. Other areas included submission of forged documents by the candidate, identification of blacklisted companies which issues fake experience letters to candidates, documents submitted by candidates for organizations which do not exist, previous employers not registered with any regulatory authority, negative performance feedback received on candidate, data theft by candidate, disconnect in company's domain name added with candidate not providing all documentations, TDS not filed by employer for entire period, further TAN was not available, mismatch in tenure of employment or designation of candidate.



Within the constantly changing terrain of the IT industry, where quick turnaround time is of utmost importance, the process of background verification stands as a critical instrument for assembling a dependable and credible team. It's a fundamental procedure that enables companies to prosper while maintaining their core values. The focus is on protecting the work environment, upholding ethical standards, and making judicious recruitment choices. This principle applies equally to large-scale international tech firms as well as emerging startups

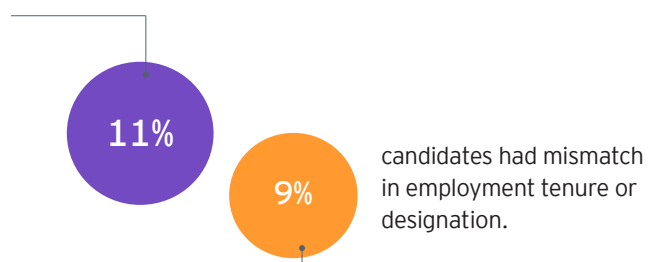
Vivek Aggarwal, Partner, EY Forensic & Integrity Services

Fake employment claims

32% candidates were flagged for submitting fake documents from companies that do not exist or from companies where the employer denied issuing such documents. In case of documents from inexistent companies that were either not registered on the MCA or GST, their non-existence was confirmed by during site visits. The candidates were unable to submit documents in majority of the cases nor would they provide UAN-linked consent.

In some instances, the company's domain name led to suspicions about its authenticity that were confirmed during site visits where no entity by the said name was found. Even the tech-skilled candidates make some errors while submitting their onboarding documents, which may not be visible to unaided vision. During these cases, using a tech-enabled document authenticator tool not only identifies fraudulent documents, but also saves the organizations from potential reputational and financial damage of hiring unethical employees.

discrepant profiles had either UAN of the employer missing or TDS was not filed by employer



Moonlighting

45% profiles of the ones marked as discrepant were found to be moonlighting- either through dual employment or had active GSTs associated with their provided PAN.

Behavioral issues

An employee is representative of the company's ethos and, hence, a mismatch can have dire consequences. During our checks we found profiles that had received negative feedback by the HR of previous employers, where the applicant was accused of absconding, data theft, integrity issues, or was charged with a financial penalty subject to civil suit.

Pending court proceedings

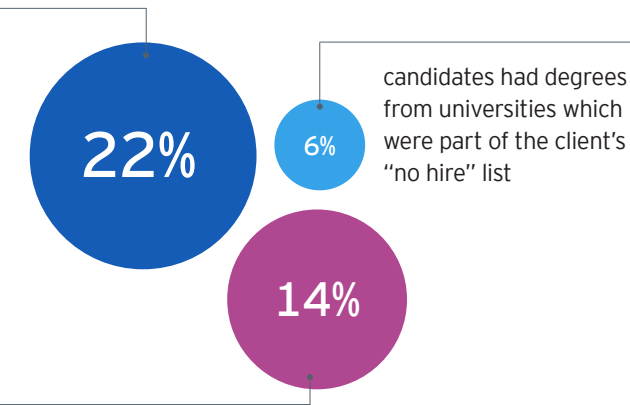
Considering that IT professionals must deal with sensitive information on a regular basis and confidentiality is key, hiring employees without conducting a criminal background check can prove to be detrimental to the companies.

During our checks, we highlighted **3%** applicants for their involvement in pending criminal or civil cases.

Embellished qualifications

Of all the discrepant profiles flagged off, **5%** were found to have embellished their educational qualifications. Since IT professionals must possess a certain level of technical acumen, failing to meet the educational requirements denotes incompetence.

candidates had failed educational qualification checks, had obtained certification from institutes categorized as “not accredited/approved” by governing bodies



candidates produced certificates from university/ college that had been accused of being involved in dubious activities in the media, rendering the candidate's qualifications insufficient for the job

In conclusion:

Tech firms frequently manage confidential information, ranging from exclusive algorithms to personal client details. Verifying that staff members have clear histories is crucial for mitigating the risk of data leaks and internal security threats, thus promoting a safer workplace atmosphere. Background screenings serve as a protective measure, thwarting possible disclosures and infringements that might damage the business and its clientele. In the current era of extensive connectivity, the standing of a company is pivotal to its triumph. Through meticulous background investigations, enterprises can steer clear of employing persons with past instances of dishonest or illicit conduct, thereby safeguarding their reputation and trustworthiness.

Analysis based on:

The data used in this analysis was sourced from over 90 organizations, primarily large-sized companies, with a few medium-sized ones included. The timeline for the data spans one year, from January 2024 to January 2025



Contact us

Arpinder Singh

Global Markets and India Leader
EY Forensic & Integrity Services
arpinder.singh@in.ey.com

Vivek Aggarwal

Partner
EY Forensic & Integrity Services
vivek.aggarwal@in.ey.com

Amit Rahane

Partner
EY Forensic & Integrity Services
amit.rahane@in.ey.com

Pushpreet Singh

Director
EY Forensic & Integrity Services
pushpreet.singh@in.ey.com

Harshita Saraogi

Senior Manager
EY Forensic & Integrity Services
harshita.saraogi@in.ey.com

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram, Haryana - 122 003, India.

©2025 Ernst & Young LLP. Published in India.
All Rights Reserved.

EYIN2504-022
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com/en_in