greenhouse

The recruiter's guide to candidate fraud

What's inside

Over the past few years, recruiting teams have noticed a shift

412%

increase in applications per recruiter from 2022-2025

Resumes are more polished and more uniform. Interviews feel unusually rehearsed. Occasionally, something about a candidate simply doesn't align.

Recruiters have always managed exaggeration, inflated titles and overstated accomplishments. It's familiar territory.

What is emerging now is different

Recruiters are now experiencing **candidate fraud.** Beyond embellishment, they're now faced with deliberate identity manipulation inside the hiring process. This is a big problem for all organizations and no longer just a theoretical possibility. It's appearing in real pipelines, and it carries implications beyond an impact on hiring quality.

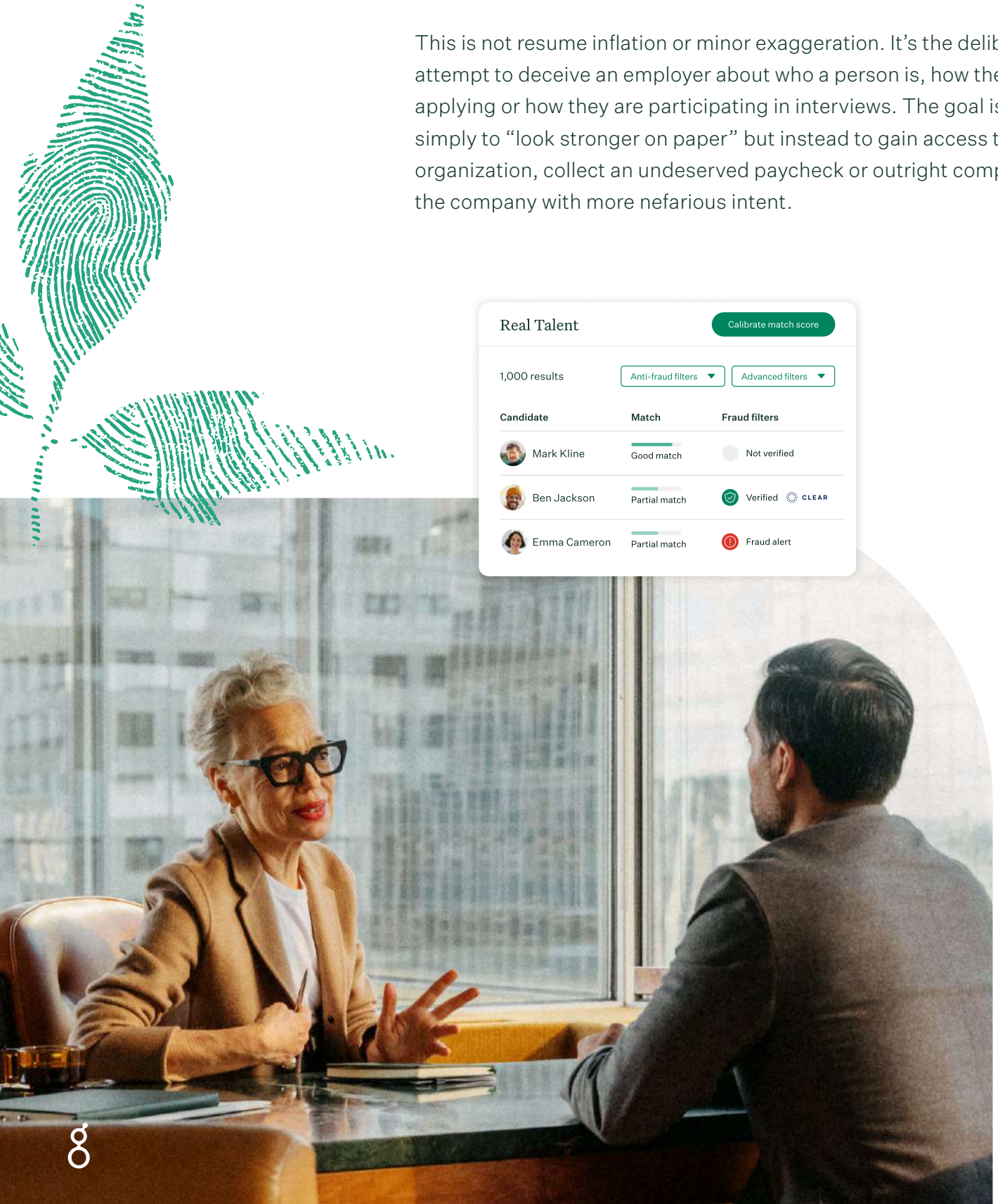
Section 1

Candidate fraud, defined

What is candidate fraud?

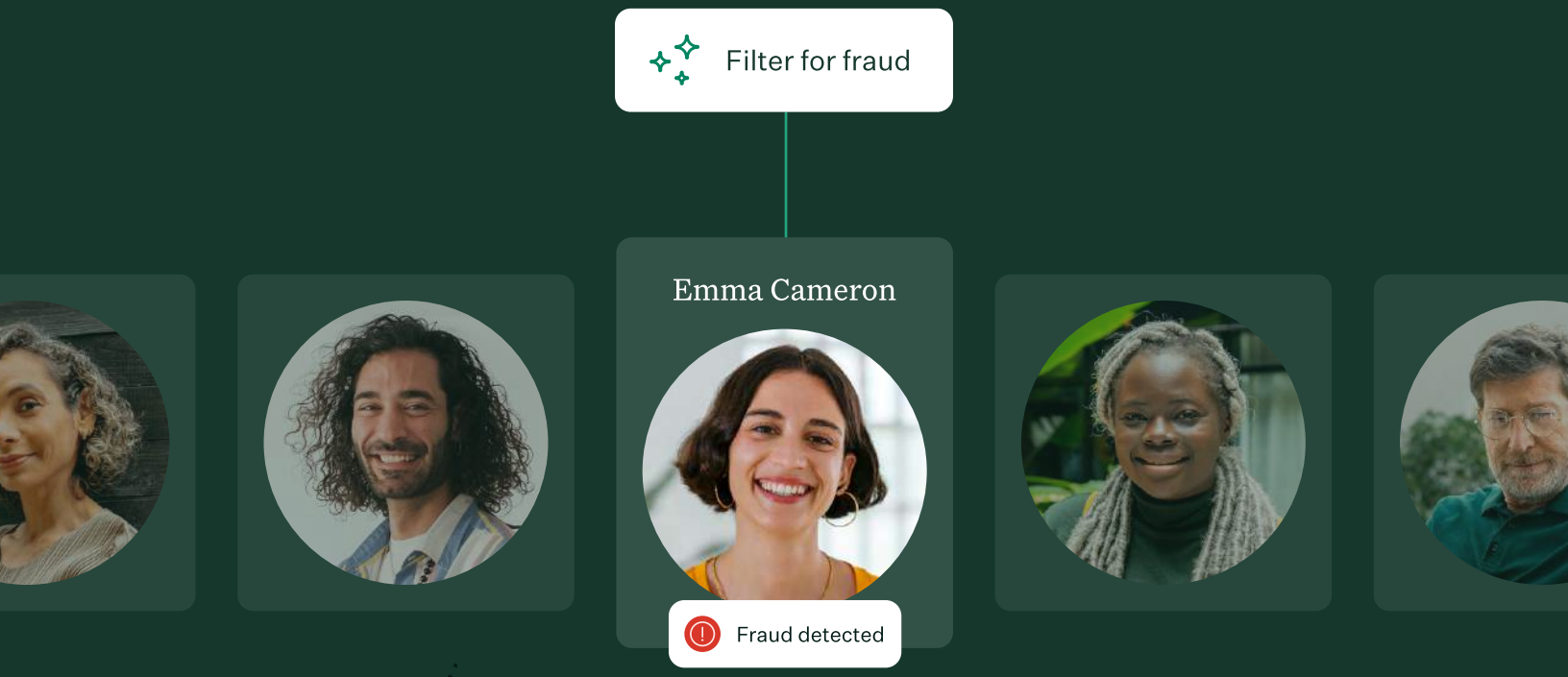
Candidate fraud is the intentional misrepresentation of identity during the hiring process.

This is not resume inflation or minor exaggeration. It's the deliberate attempt to deceive an employer about who a person is, how they are applying or how they are participating in interviews. The goal is not simply to "look stronger on paper" but instead to gain access to an organization, collect an undeserved paycheck or outright compromise the company with more nefarious intent.



Types of candidate fraud

Candidate fraud can take several forms, each carrying its own risk and potential consequences. By understanding the differences, teams can recognize patterns early before any damage is done.



1. Synthetic identities

Fraudsters combine real and fabricated information to create a new identity.

This may involve:

- A legitimate Social Security number paired with a different name
- AI-generated profile photos
- Fabricated work histories that align convincingly with the role

These identities can pass superficial checks because they are partially real or use real information.

2. Impersonation

In these cases, someone steals the identity of a real person.

This can include:

- Hijacked LinkedIn profiles
- Stolen resumes
- Interview participation under someone else's credentials
- Credential falsification (signing into someone else's account)
- A candidate pretending to be a real person (without that person's knowledge or consent)

The employer believes they are speaking to one person when they are not.

3. Coordinated activity

Some fraud attempts are organized.

Patterns may include:

- Multiple similar applications from related or identical email domains
- Repeated IP address overlap
- Repeated interview scripts across different candidates

This operational coordination can indicate intentional targeting. In this case, the company may be specifically attacked by a criminal organization or hacker group specifically trying to gain access to that company.

4. AI misuse during interviews

AI tools are increasingly being used to.

- Generate real-time answers during live interviews
- Manipulate video feeds using deepfake technology
- Feed candidates scripted responses through hidden prompts

This misrepresents the candidates' ability to perform their job and leads to mis-hires.

Section 2

Consequences of candidate fraud

This shift is already impacting organizations

Over the past few years, we've already seen documented cases of candidate fraud that have resulted in mis-hires, data breaches and even financial losses.

Candidate fraud in the media

In 2025, Amazon security leaders disclosed that they blocked thousands of suspected North Korean job applications for remote technical roles, citing efforts to prevent state-linked actors from infiltrating internal systems.

In 2024, ITPro reported on North Korean operatives hijacking legitimate LinkedIn profiles and using them to apply for remote IT positions.

The Associated Press detailed how remote job placements have been exploited to generate revenue and access for state-sponsored operations.

The Week covered the growing use of AI tools, including real-time video manipulation, during job interviews.

Fast facts

63%

Experienced resume exaggeration

48%

Shared fake references

35%

Used AI-assisted interview responses

Candidate fraud by the numbers

What used to be occasional red flags is now a consistent pattern. 91% of recruiters say they've encountered candidate deception –most commonly resume exaggeration (63%), fake references (48%) and AI-assisted interview responses (35%).

High-profile fraud schemes have generated hundreds of millions of dollars annually and impacted hundreds of companies, including Fortune 500 organizations.

At an individual level, the cost adds up quickly. Companies report losing an average of $28,000 per fraudulent hire, factoring in investigation costs, lost productivity and remediation.

It's clear that candidate fraud is likely to get worse as fraud becomes more technologically accessible and more operationally organized, aided by AI and fueled by what bad actors can reap, such as data, paychecks and more.

When someone exaggerates their skills, the consequence is usually limited to performance and role fit. When someone falsifies their identity, the consequences can extend far beyond a single open role. At that point, hiring becomes a matter of organizational trust.

Why this matters beyond the hiring team

The impact of candidate fraud exists on a spectrum.

At the lower end, a fraudulent application wastes time. Recruiters and hiring managers spend hours screening and interviewing before realizing something is off. The role stays open longer or a mis-hire is made. Team productivity slips. Business timelines shift. This can be impactful enough for a company that is waiting on key hires to be able to deliver a key deadline or meet their customers' expectations.

But the consequences don't stop there.

At the far end of the spectrum, organizations may be deliberately targeted. A fraudulent candidate gains employment using a convincing identity and then accesses:

- Customer data
- Financial systems
- Intellectual property
- Internal infrastructure

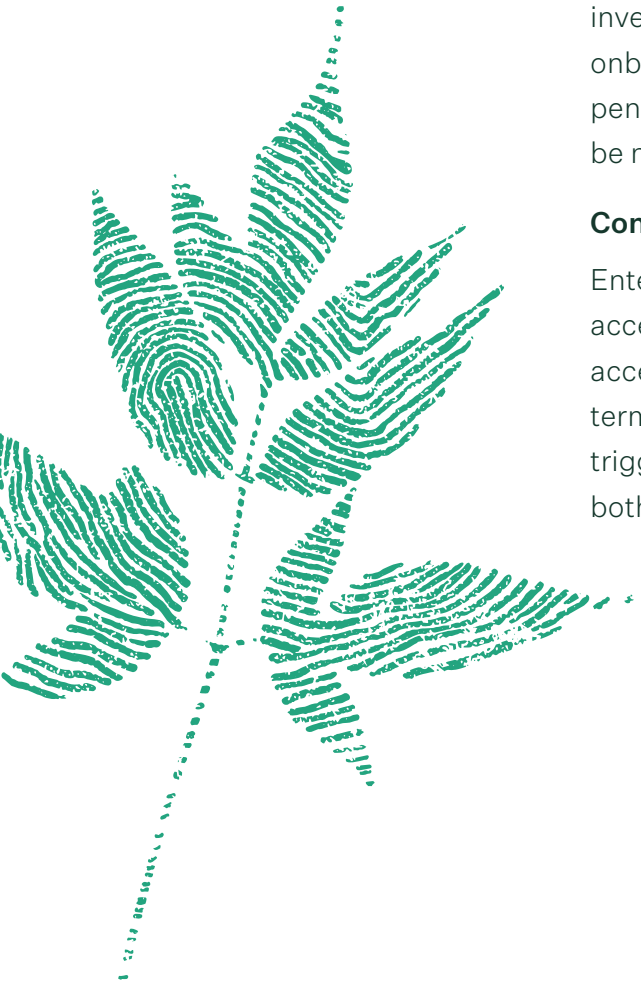
This can have disastrous consequences for a company and can include:

Data exposure and data breaches

A fraudulent hire can gain legitimate access to internal systems with elevated sophistication, making detection of improper systems access more difficult and ultimately resulting in a more severe impact. Depending on the fraudulent role, this can include customer data, financial records, proprietary code or internal documentation. Even limited access can be enough to copy, transfer or slowly exfiltrate sensitive information over time. In many cases, this triggers formal breach investigations and internal audits, which can have downstream impacts on operations, reputation and revenue.

Regulatory and compliance scrutiny

In regulated industries, identity verification is expected. If a fraudulent individual gains access to sensitive systems, regulators may investigate whether proper controls were in place during hiring and onboarding. This can lead to audits, compliance reviews and potential penalties, which can get worse if the affected organization is found to be negligent.



Contract violations

Enterprise agreements often include strict requirements around data access, employee vetting and security controls. If a fraudulent hire accesses customer or partner environments, it may violate those terms. Organizations may be required to notify affected customers, trigger security reviews or renegotiate contractual obligations, putting both revenue and relationships at risk.

Operational disruption

Depending on the intent, some candidate fraud may be seeking to specifically disrupt business operations. This can be done by accessing key systems and turning them off, removing access to accounts and more. Detecting and identifying the scope of the damage often requires multiple teams and a heavy investment in resources, especially if a forensic investigation is required. These efforts can take days or weeks, pulling multiple teams away from core priorities and slowing down the business.

Reputational damage

Trust is difficult to rebuild. If customers, partners or the public learn that a fraudulent actor gained access through the hiring process, it can raise concerns about internal controls and oversight. Even if the incident is contained, the perception of vulnerability can impact customer confidence, brand credibility and future business opportunities.

Section 3

The recruiter and candidate fraud connection

The increasing role a recruiter plays in managing candidate fraud

Recruiters are now the first line of defense when it comes to candidate fraud.

Security teams do not screen resumes.
IT does not conduct interviews.
Legal does not evaluate candidate behavior in early stages.

This means recruiters need to be the ones to spot or flag any suspicious behavior such as:

- Repeated inconsistencies across applications
- Interview behavior that does not align with claimed experience
- Suspicious patterns across multiple candidates

However, due to recruiters' overwhelming demands, they may not have the time, resources or expertise to truly assess the risk candidate fraud poses to an organization. Higher application volume, leaner staffing. Increased expectations already demand a lot from recruiting teams. But just because recruiters can't always assess the risk of candidate fraud, that doesn't mean the risk is eliminated.

Candidate fraud does not mean recruiters need to become investigators, but they do need to understand how to address this role shift. Recruiters are now responsible for both talent quality and an early layer of organizational trust. That means closer collaboration with Legal, IT and Security – and a new category of work that didn't exist before.

How recruiters can spot candidate fraud

Most fraud doesn’t reveal itself all at once.
It shows up in small inconsistencies across the hiring process.

Here are common signals recruiters are already seeing:

Application stage signals

- Resume formatting or phrasing that feels overly uniform across multiple candidates
- Mismatches between resume details and LinkedIn profiles
- Unusual email domains or slight variations of legitimate company name
- Multiple candidates sharing similar work histories, timelines or bullet points

Screening stage signals

- Answers that feel overly polished but lack depth when probed
- Difficulty explaining specific decisions, trade-offs or real-world examples
- Inconsistencies when revisiting earlier answers
- Delays or pauses that suggest reliance on external tools

Interview stage signals

- Camera avoidance or reluctance to turn on video when expected
- Lip sync issues, unnatural eye movement or delayed responses (possible AI assistance)
- Strong theoretical answers but weak applied knowledge
- Different communication styles across interview stages

Pattern-level signals

- Repeated interview scripts across multiple applicants
- Similar responses, phrasing or examples across candidates
- Coordinated timing of applications

Validating without bias at the interview stage

Spotting signals is only the first step. The goal is to validate without introducing bias or breaking the candidate experience.

Recruiters and interviewers can:

- Ask candidates to walk through specific past decisions ("What trade-offs did you make?")
- Introduce follow-up questions that require real-time thinking
- Request live problem solving or scenario-based exercises
- Revisit earlier answers later in the process to check for consistency
- Ask candidates to explain how they approached a problem, not just the outcome

These techniques make it harder to rely on scripted or assisted responses, and easier to identify authentic experience.

Quick checklist for recruiters

If something feels off, pressure-test it:

- ☐ Can they explain their experience in detail?
- ☐ Are answers consistent across interviews?
- ☐ Do resume, profile and behavior align?
- ☐ Are patterns appearing across candidates?

If not, it's worth a deeper review.

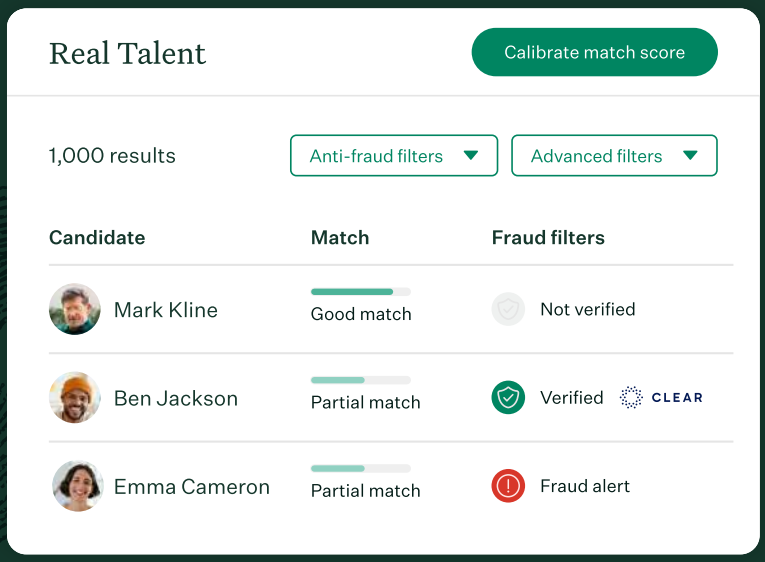
Section 4

Navigating candidate fraud at the individual and organizational level

Managing candidate fraud as an organization

Managing candidate fraud doesn't require a complete overhaul of your hiring process. Instead, reinforcing structured practices, maintaining foundational elements to hiring and adding intentional safeguards go a long way without requiring a massive resource or timing investment.

A triple-layer approach works best.



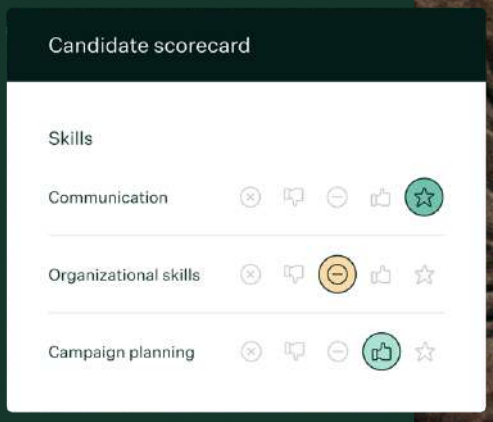
01.

Strengthen structured hiring practices

Structured hiring improves fairness and performance. It also reduces fraud risk by reducing ambiguity, which can fuel fraud efforts.

Recruiters can implement this by:

- Defining clear competencies for every role
- Using standardized interview scorecards
- Requiring documented evidence for evaluations
- Training interviewers to probe for applied experience, not theoretical knowledge



02.

Surface objective fraud signals early and establish communication strategies

Fraud signals often exist, but they are fragmented. By having a collective view of these disparate signals, recruiters can identify patterns and more confidently flag a potential issue.

Recruiters can:

- Standardize how suspicious patterns are documented
- Establish a simple escalation path with Security or IT
- Create internal guidelines for red flags
- Leverage tools that surface objective indicators within the hiring workflow

These signals may include:

- IP inconsistencies
- Email domain mismatches
- Repeated resume structures
- Profile discrepancies

The goal is not automatic rejection.
It is visibility and consistency in review.

03.

Introduce identity verification at appropriate stages

For higher-risk roles or later stages of hiring, identity verification can serve as an additional safeguard. Confirmation that a real person is behind an application adds another layer of confidence, particularly in remote-first environments where physical presence is rare or not possible.

Recruiters can:

- Request live ID confirmation for high-risk roles
- Conduct structured live technical assessments with camera requirements
- Align with IT or Security on when additional verification is appropriate
- Use third-party verification tools when risk level warrants it

Verification should be intentional and role-based, particularly for:

- Remote technical positions
- Roles with system access
- Positions handling sensitive data

Identity confirmation adds confidence in environments where physical presence is absent.

In the field: How teams are actually navigating candidate fraud

Organizations that have formalized a more structured approach to candidate fraud consistently describe two shifts: less manual work and greater confidence identifying fraudulent candidates earlier in the hiring funnel.

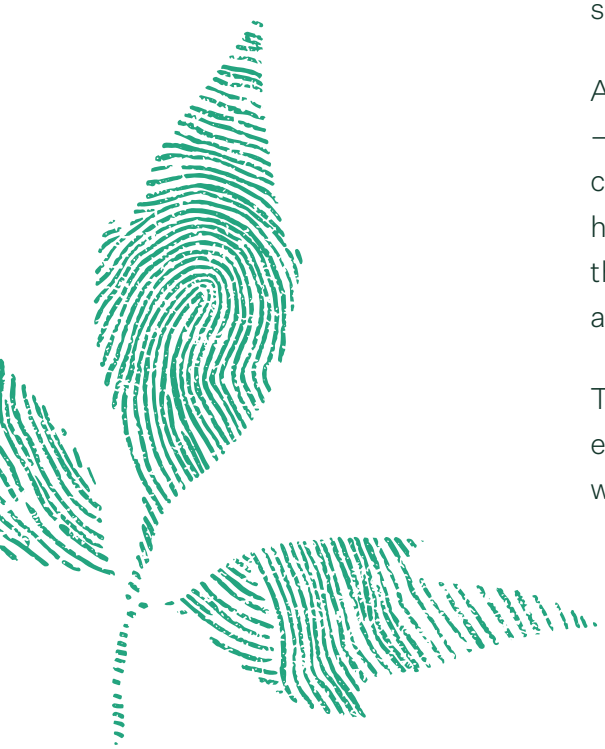
BambooHR's Talent Acquisition Operations lead described candidate fraud detection as a major operational improvement because it "centralized the fraud checking effort in the applicant tracking system (ATS), reducing the time spent in app review."

That operational lift matters because many teams were previously piecing together signals manually across spreadsheets, reverse lookups, IP checks and multiple external tools.

BambooHR also reported a quality benefit, citing "an increase in the authenticity of candidates' identities and an increase in our ability to spot fraud candidates at the top of the funnel."

At the same time, teams are clear that visibility alone is not enough – especially as fraud tactics continue to evolve. As one prominent cybersecurity Greenhouse customer puts it: "Fraudsters will always have new tricks. It's a lot of burden on recruiters to know how to read those fraud signals together, especially as tricks evolve. Recruiters aren't IT experts."

That is the balance teams are looking for: stronger signals, clearer explanations and workflows that help recruiters act with confidence without turning them into security analysts.



What to be cautious of

As candidate fraud becomes more visible, the market will respond with new solutions and bold claims. However, not all tools or platforms can deliver on their promises and leaders should be cautious when considering a partner that can help them and their team manage candidate fraud.

Recruiting leaders should be cautious of tools that:

Promise definitive fraud detection without explainability
If a system flags or rejects a candidate, teams must understand why. Black-box decisions create compliance and fairness risks.

Replace human decision-making entirely
Automated disqualification without review can create bias exposure and regulatory vulnerability.

Conflate resume quality scoring with identity verification
Evaluating skill alignment is not the same as confirming identity. These are separate controls.

Lack audit trails
In regulated industries, teams must be able to demonstrate how decisions were made. Documentation and transparency are critical.

Transparency and oversight are not optional when it comes to managing candidate fraud, and detection must be defensible. Otherwise, false positives may heavily impact the candidate experience, ultimately resulting in negative hiring outcomes.

Conclusion

The new reality

Recruiting already operates under leaner teams, higher application volume and increasing expectations around speed and quality. Candidate fraud adds another layer, but it does not require a fundamentally new discipline.

It requires layered trust, which is only possible with structured processes, clear documentation, alignment with Security and Legal and thoughtful use of tools that support, rather than replace, human judgment.

Recruiters have always been stewards of talent quality, and now they are also part of protecting organizational trust. This is a new responsibility, but with the right layers in place, it is entirely manageable.

Want to know what to do next?

To understand more about how Greenhouse can help you manage candidate fraud with Real Talent™, book a demo.

greenhouse

Greenhouse is the leading hiring platform to help companies get measurably better at hiring. Our AI-powered software supports every stage of the hiring process, from sourcing to onboarding, giving businesses everything they need to hire top talent quickly, consistently and fairly – today and as their business grows.

To learn more, visit

greenhouse.com