greenhouse

The TA guide to working with legal and security

A practical partnership for the age of fraud and AI risk

Hiring risk is new, and no one handed you a playbook

You're three interviews deep with a candidate who looks perfect on paper. Still, something is off. The answers are a little too smooth, the details are a little too thin and a quiet voice says to loop in security. A louder one says you'll blow up your timeline over a hunch. So you keep going. Most recruiters would.

A few years ago that hunch meant a padded resume. Now it can mean an organized group looking to target your company's data. Candidate fraud at this level barely existed before generative AI made it cheap and fast, which is exactly why it catches good teams off guard. The threat now runs on a spectrum.

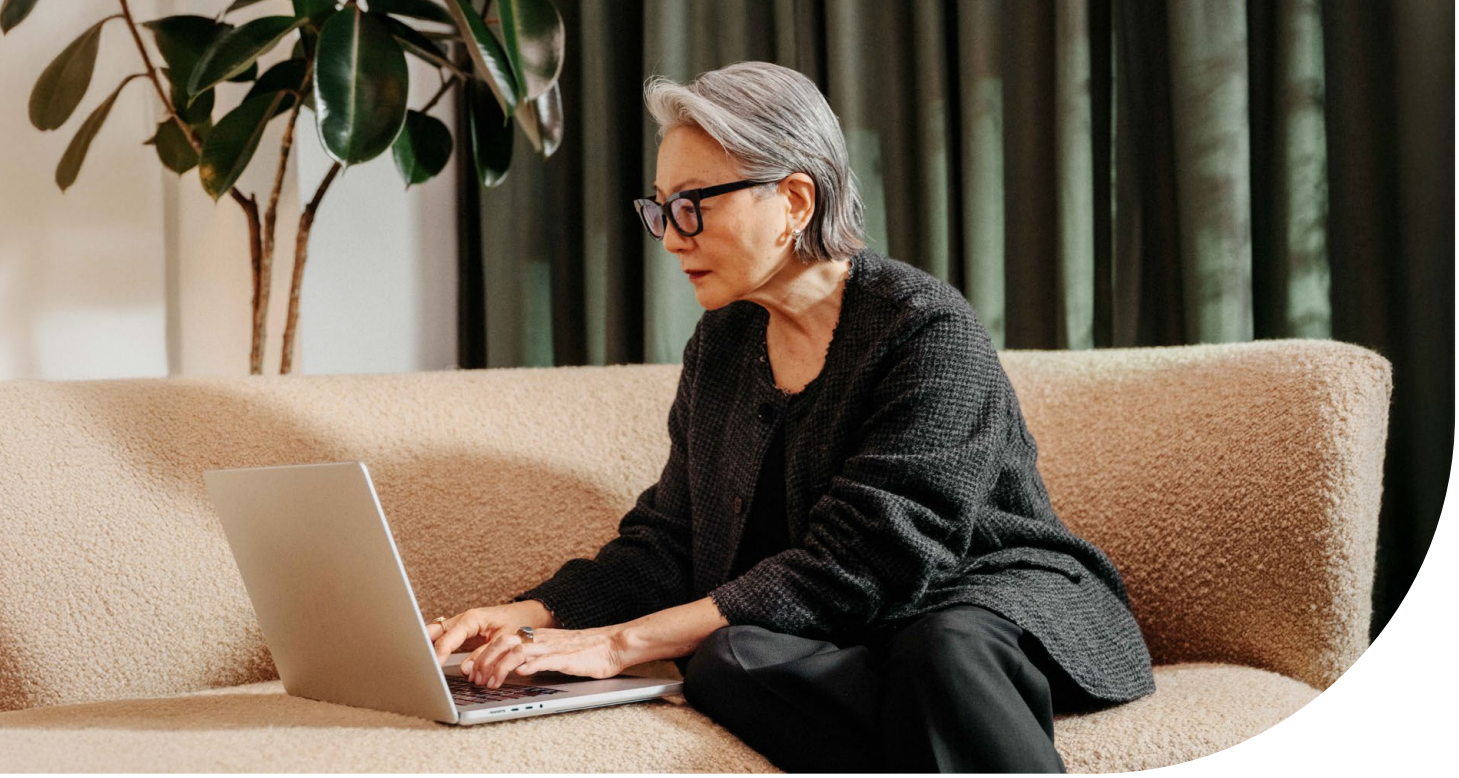
Three-tier threat band

Low – Interview cheating and dual employment: Workers cheating through interviews or juggling secret second jobs.	**The result:** Wasted recruiting effort and hires who never perform.
Medium – Worker farms and fake personas: Offshore operations fake their location and send a "ringer" to interview while someone else shows up on day one.	**The result:** A paycheck and system access handed to someone you never verified.
High – State-sponsored and independent hacking groups: Actors who get hired specifically to reach your systems, data and customers.	**The result:** Your systems and data get exposed from within. Think data breaches, investigations and a massive business disruption.

AI tools: Regulations and governance

Fraudulent candidates are only half of it. The moment an AI tool screens, ranks or scores candidates, it's making decisions a candidate could challenge. Frameworks like the EU AI Act treat that as high risk, requiring explainability, human oversight and candidate transparency. Get it wrong and the exposure is yours, not the vendor's.

As you interact with AI tools and consider new ones for your team, knowing how they interact with regulatory and compliance requirements is likely a question you'll be asked often. Preparation goes a long way to speedy and effective implementation.



91%

of recruiters have encountered candidate deception

$28K

average cost of a single fraudulent hire

$100M+

lost annually to organized fraud schemes targeting large companies

So risk runs two ways: fraudulent candidates and the AI tools you bring in. Both land on TA. Because it's all new, most teams improvise – vetting alone, staying quiet until they're certain and trying to figure it all out when it's too late. Each of those shortcuts trades a little time saved now for real exposure later.

The stronger move starts with your role. TA owns the outcome, but you don't have to own the process alone. You decide what a defensible hire looks like – and you lean on legal and security to spot the risk signals and to know how to flag them when they surface.

This guide shows you how – giving **recruiters** a clear rule for when to escalate and a fast way to do it, and giving **TA leaders** a way to set guardrails up front and bring legal and security in from the start, so protection is ready before risk shows up.

Collaboration starts before the crisis

The worst time to work out how to collaborate with legal and security is mid-crisis – staring at a suspicious candidate or halfway through an AI vendor demo that starts to raise some flags. Agree on how you'll handle the two most common situations, so the path exists before you need it.

Settle these upfront and you can flag a risk or pause a vendor with confidence, without wondering if you're overreacting.

When you suspect application fraud

1. **Agree on what to raise.** Bring a starting list and let legal and security turn it into criteria that fit your business:
   - An identity that doesn't line up across sources (LinkedIn, resume, etc.)
   - Candidate from a later round is different from who you screened
   - Employers or references from companies that seem fake or can't be verified as real
   - A hunch you cannot back up yet (uncertainty is enough to loop someone in)
2. **Agree on the communication.** Decide how a flag travels – a ticket, a Slack channel, a shared inbox – so it's fast and on the record.
3. **Agree on the action you take.** Settle what a recruiter does the instant they flag something wrong: pause the candidate, note what they saw, wait for alignment before acting.

When assessing an AI hiring tool

1. **Agree on what needs sign-off.** Settle which uses you can run with, and which need a full review first. You might need sign-off on the below:
   - Automated ranking or decisions that advance or reject a candidate
   - Tools that mix identity verification with risk scoring, so you can't tell what's actually being checked
   - Fraud detection that claims to be fully automated, with no human review of the flags
   - Any tool that can't show an audit trail or hasn't had a recent bias audit
2. **Agree on who to call,** in what order. This is usually legal on the use case, then security on the vendor, but get alignment from the respective teams first.
3. **Agree on your bar.** Ask your security and legal teams what vendor criteria is necessary – explainability, audit trails, hiring-specific signals, candidate rights – so a tool that can't meet them is an easy no.

From plan to action

You've now set the ground rules. Here's how they play out when the moment actually arrives – a suspected fraud case, and bringing in an AI tool.

Resist the instinct to confirm it yourself before looping anyone in. Fraud gets easier to handle the earlier you share it.

Guide for suspecting fraud

1. **Pause the process.** Don't advance the candidate and don't tip them off.

2. **Document what you see, now.** Capture the specific signals while they're fresh, in the ATS.

3. **Raise the flag** through your agreed channel. Keep your comms short but on the record. Regulations require an audit trail, so update all conversations in your ATS.

4. **Bring together** legal, security (and HR, if necessary). Stay the owner until you hear otherwise. Convene the thread and make sure each team is clear on what pertains to them – you keep the record. (See table on next page)

5. **Decide together, then act.** No one contacts the candidate until the group agrees on how. You may want to confront a suspicious candidate yourself – don't. Ensuring fraud can't reach your organization is paramount to addressing it, so you don't want to scare away a suspect without getting all the facts first.

Here's what to flag to key teams

Team	What you hand them	What they should provide
Security	What you observed – the mismatch, the switched candidate, whatever felt off – with a request to take a closer look.	A check on the signals you can't see – device, location, proxy, account history – and whether they add up to a real threat.
Legal	The facts, timeline and any additional context. This can include what happened, when and what stage the suspected candidate is in.	An assessment of your exposure (employment, privacy, contractual) and the options you can act on.
HR	Ideally, you'd flag before it gets to this point, but if an offer has gone out, provide HR with the employment context.	The people-and-process communication path and criteria on when you should reach out to HR next time.

Pro tip

Document defensibly: Your notes are what the whole team works from

Every team you bring in relies on the record you keep. Document in your ATS as you go so security, legal and HR are all working from the same facts – not your memory of them.

- **Do:** Keep notes contemporaneous – written while they're fresh. Keep everything in your ATS or within your company's communication channels.
- **Don't:** Edit or delete notes after the fact, or move discussions to off-record personal channels.

> "The single most important thing when fraud is suspected is documentation – structured scorecards, timestamps, what was said in each interview."

Cian Martin
Director of Legal, EMEA, Greenhouse

When you roll out an AI hiring tool

The same principles apply here. Sort out how you'll work together early – who to bring in, and what actually calls for a legal or compliance review – so you have a frame of reference each time a new tool comes across your desk.

Guide for rolling out an AI tool

1. **Define the outcome and guardrails** for the tool. What it's for, where a human decides, what a candidate can opt out of (if it's candidate facing).
2. **Bring the pre-brief to legal and security** at scoping – not after you've picked a vendor. If a vendor can't meet what they require, that's your answer and you keep looking (see table below).
3. **Confirm explainability and audit trails.** It's a red alert if your AI tool isn't able to produce these.
4. **Document the sign-off.** Capture the review so the rollout is defensible long after launch.

> "For anything involving employment and AI, my first call is to both Legal Risk and Employment Legal. Then I loop in security and our CISO, whose team runs the tool review, so I learn their vendor questions up front. If a vendor doesn't have those things in place, I already know we likely won't move forward."
>
> **Erin Walsh-Beguin**
> Senior Director, Global TA Ops, GoDaddy

Your AI tool pre-brief

Team	What you bring them	What they help you lock down
Security	The outcome you want and how it touches candidates or your company data.	Whether it's compliant in the jurisdictions you hire in, and what kind of candidate transparency, opt-out process and data management you need in place.
Legal	The vendor and the tool itself: what data it would touch, how it's built and how it reaches a result.	The kind of data that a tool uses and whether that's worth bringing in security to conduct due diligence on their side.

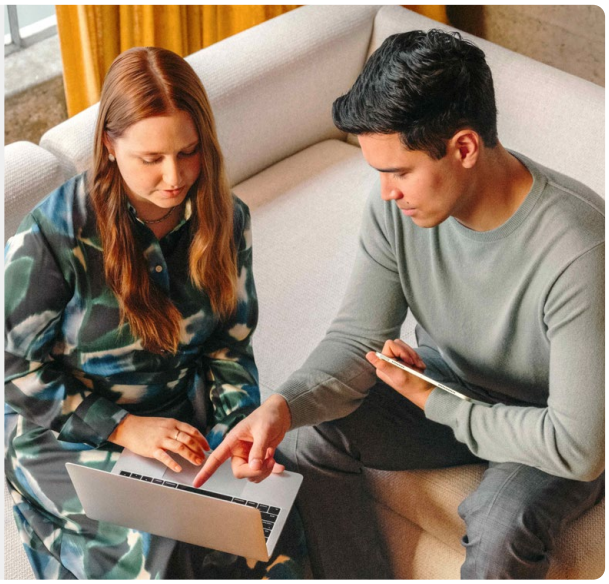
This is a conversation, not a gate

If you take one idea from this guide, let it be that working with legal and security isn't a checkpoint you clear at the end. Instead, it's an ongoing conversation you start early and keep open.

And the one action worth building into every hire: **when in doubt, raise it.** You don't have to be certain. You don't have to have it figured out. Raising your hand early is what protects your speed and your process at the same time.

Start here this week

- ☐ **Sit down with legal and security** to agree on what to raise and what needs sign-off, before the next case or tool.
- ☐ **Agree on an escalation channel** with your legal and security partners, so raising a flag takes seconds.
- ☐ **Move any off-platform candidate** conversations back into your ATS – not personal email or messaging apps – so the record stays auditable in one place.



The takeaway

Fraud and AI risk aren't going to slow down, and neither can you. The teams that hire fast and stay protected share a few habits: they bring legal and security in early, they build defensibility into how they work and they treat risk as a shared responsibility. Start the conversation before you need it and it stops being a brake and becomes a foundation.

See how Greenhouse Real Talent™ builds fraud signals, audit trails and explainable rankings into your process – so you catch more, escalate with evidence and keep every decision in human hands.

Learn more

Contributing experts

Erin-Walsh Beguin

Sr. Director, Global Recruiting Operations & Employer Brand, GoDaddy

Erin Walsh-Beguin is Sr. Director, Global Recruiting Operations & Employer Brand at GoDaddy, where she's worked since 2017. She serves on the Greenhouse Customer Advisory Board, focusing on recruiting tech, compliance and employer brand.

Generi Wilson

Talent Acquisition Program Manager, Greenhouse

Generi is Talent Acquisition Program Manager at Greenhouse, designing and operationalizing hiring programs that help Greenhouse attract, engage and hire top talent at scale. The first to hold this role, she's launched initiatives that set the industry standard for great hiring practices.

Cian Martin

Director of Legal, EMEA, Greenhouse

Cian is Director of Legal, EMEA at Greenhouse, leading legal strategy across the region. A seasoned in-house counsel, he previously held senior legal roles at Benchling, Twilio, IAC and Segment. Cian began his career at a leading Irish law firm advising global teams on regulatory matters.

Jung-Kyu McCann

Chief Legal Officer, Greenhouse

Jung serves as Chief Legal Officer at Greenhouse, managing all legal and compliance matters. She previously was CLO and Interim CPO at Druva, and held legal roles at Apple and Broadcom. Jung also serves on the Board of the Society for Corporate Governance and the Women's General Counsel Network.

Ron Gutierrez

Senior Director of Security, Greenhouse

Ron is Senior Director of Security at Greenhouse, leading product, corporate and information security while partnering on AI and fraud initiatives like Greenhouse Real Talent™. He previously led security for PayPal's Venmo business and was a technical lead at a security consulting firm.

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