

THE COST OF DOING NOTHING

What Unverified Identity Costs Enterprises Every Year

An industry-by-industry breakdown of the operational, financial, and security costs enterprises pay every year for trusting that the person behind the account is who they claim to be.

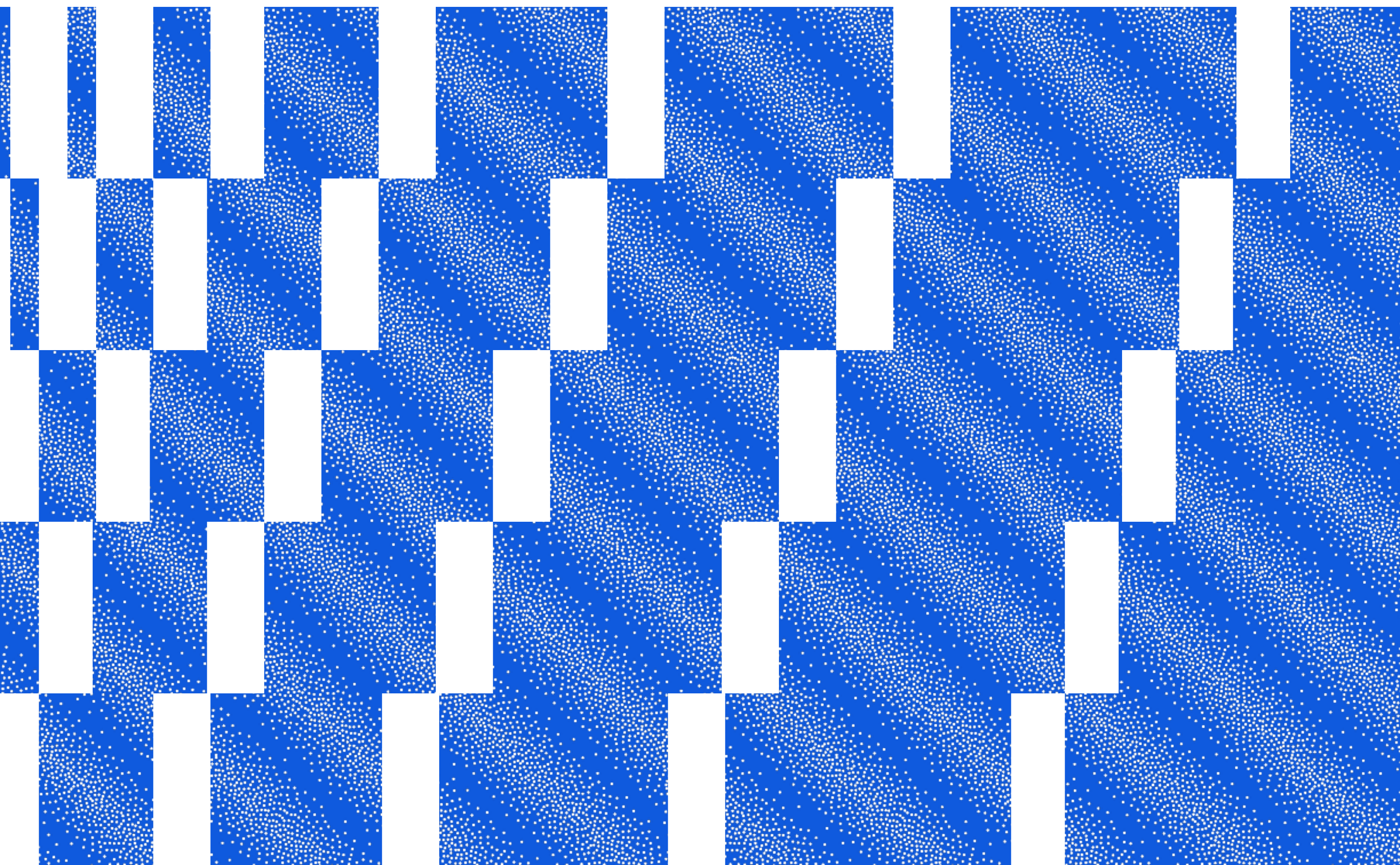


Table of Contents

Executive Summary	01
The Identity Threat Landscape	02
Four Ways Inaction Shows Up on Your Books	04
Operational Efficiency	04
Workforce Productivity	05
Annual Loss Expectancy	07
Hiring Fraud	09
What Doing Nothing Costs By Industry	11
Healthcare	13
Technology	15
Hospitality, Retail & Consumer	17
Industrial Manufacturing	20
Education	22
Transportation	25
The Compounding Effect	28
From Cost to Control: How to Close the Gap	29
Methodology	30

Executive Summary

Across every enterprise, high-risk workforce actions are being authorized on the assumption that the human with the right credentials is who they claim to be. Identity infrastructure was built to confirm which account is acting. It cannot confirm which human is acting. That gap is the most expensive line item most organizations have never measured.

AI has dropped the cost of convincing impersonation to near zero, while the controls most enterprises rely on were built to verify accounts and credentials, not the people behind them.

The cost compounds across four dimensions, each owned by a different executive and each paid simultaneously. Operational efficiency. Workforce productivity. Annual Loss Expectancy. Hiring fraud. Stacked across 12 months for a 15,000-employee organization, those four costs total roughly \$7.8M. Enterprise Identity Verification (IDV) recovers roughly \$6.5M of that net of license cost. Break-even is measured in weeks.

The most useful way to read these numbers is by the week. Healthcare carries roughly \$150,000 a week in accumulated identity exposure. Technology, \$134,000. Industrial Manufacturing, \$126,000. The annual figure is the headline. The weekly rate is what makes the cost of waiting feel like what it actually is.

The chapters that follow quantify each cost dimension in detail and translate them into industry-specific exposure across six sectors: Healthcare; Technology; Hospitality, Retail & Consumer; Industrial Manufacturing; Education; and Transportation. The figures are calibrated to give each executive an order-of-magnitude view of what the gap is currently costing their organization.

Four dimensions, paid at once

Each cost carries a label, a one-line description, a headline figure, and the executive who owns it.

Operational Efficiency	Workforce Productivity	Annual Loss Expectancy	Hiring Fraud
The IT labor and overhead burden of running manual identity verification.	The hours employees lose to identity friction, valued at fully loaded compensation.	The actuarial financial exposure tied to identity-driven breaches.	The identity risk that enters the organization before an employee's first day.
\$1.25M	\$1.92M – \$4.48M	\$1.27M – \$4.97M	\$1.19M
Annual cost at scale	Annual cost range	Annual cost range	Operational cost up to \$26.7M OFAC sanctions liability, per fraudulent placement
OWNS IT: CIO	OWNS IT: CIO AND CTO	OWNS IT: CISO AND CFO	OWNS IT: CFO, CEO, AND GENERAL COUNSEL

Figures are illustrative for a 15,000-employee organization. The four costs are paid simultaneously, not in sequence. Total annual cost of inaction at this workforce size ranges from \$4.12M to \$7.8M depending on industry, before OFAC liability is layered on.

The Identity Threat Landscape

For more than two decades, security investment focused on hardening the perimeter — firewalls, endpoint protection, network segmentation, patch hygiene. That work matters, but it is no longer where most breaches start. Sophos analyzed 661 incident response cases between November 2024 and October 2025 across 70 countries and 34 industries. Identity-related root causes drove 67% of every successful intrusion. The pattern was consistent across every vertical, every regulatory regime, every geography. The attackers are not breaking in. They are logging in.

The attackers are not breaking in. **They are logging in.**

That shift has an economic explanation: it is cheaper to use a working credential than to develop a new exploit. Compromised credentials alone accounted for 42% of all root causes. A valid username and password pair was already in the attacker's possession before the incident began.

The 2026 Cloudflare Threat Report confirms how cheap that asset has become. 63% of all logins now involve credentials already compromised elsewhere. 94% of all login attempts originate from bots, not humans. A working credential is no longer a rare find. It is a commodity.

The standard answer to credential compromise has been multi-factor authentication. Sophos found MFA absent or misconfigured in 59% of identity-related incidents. Where it was deployed correctly, attackers adapted. Adversary-in-the-middle proxies intercept authenticated sessions after MFA completes. Infostealer malware extracts active session tokens that bypass authentication entirely. Authentication confirms a credential, not the person behind it.

This gap expands beyond employees. Contractors and suppliers move through the same identity stack. In their 2026 Annual Threat Report, Darktrace investigated breaches at Jaguar Land Rover, Marks & Spencer, and Salesforce in 2025 — none began with a software exploit. All began with compromised identity. Once inside, attackers used trusted accounts and existing permissions to operate in plain sight. The recovery flow that can reset a sales rep's password can also reset a third-party developer's access to production.

AI is widening the gap. Darktrace tracked more than 8.2 million phishing emails targeting VIPs in 2025 — over a quarter of all phishing activity in that period. Cloudflare documented state-sponsored operatives using deepfakes to infiltrate Western payrolls through fake employment. AI lowers the cost of impersonation while raising the cost of detection.

Identity Maturity Framework

Where an organization sits on the verification maturity curve determines how much of the workforce identity gap is closed.

Stage 1 — Manual Verification	Human judgment, no automation. The full ALE is carried.
Stage 2 — Compliance-Grade Verification	Point-in-time selfie matching, custom integration logic, significant developer maintenance burden. Retains 50–60% of baseline ALE.
Stage 3 — Security-Optimized Verification	3D liveness, cryptographic device binding, identity orchestration. Reduces residual exposure to 15–25% of baseline.
Stage 4 — Managed Enterprise Verification	Continuous assurance across the workforce lifecycle, vendor-managed edge case resolution, expert-managed appeals. Reduces residual exposure to single digits as a percentage of baseline.

Most organizations sit at Stage 2. The cost of waiting is the difference between Stage 2 and Stage 4, multiplied by every week the gap remains open.

AI Agents and the Authorization Question

Enterprise AI agents act on credentials. They authenticate as a human user, hold the same access rights, and execute workflows that move money, change records, and grant access.

When an agent's action triggers a high-consequence outcome, the question of who authorized it has to be answerable.

The verified human layer that closes the workforce identity gap is the same layer that makes AI agent actions accountable.

The work most enterprises have done is real. MFA is deployed, the IdP is in place, the helpdesk has a runbook for password resets. That foundation has held up well, but the threat landscape has continued to shift. Authentication confirms an account; the next layer of defense has to confirm the human.

The cost of leaving this gap open is not theoretical. It is operational, financial, and accumulating right now.

Four Ways Inaction Shows Up on Your Books

The cost of workforce identity risk is not a single line item. It is accrued in four places:

- 1. **Operational Efficiency:** the IT labor and overhead burden of running a manual identity verification operation
- 2. **Workforce Productivity:** the hours employees lose to identity friction across the workforce
- 3. **Annual Loss Expectancy:** the actuarial financial exposure tied to identity-driven breaches
- 4. **Hiring Fraud:** the identity risk and recruiting cost that enters the organization before an employee's first day

Each is real. Each is current. The total is almost always larger than anyone in the room expects. Seen together, the four numbers tell the real story.

Operational Efficiency

The cost of helpdesk identity verification rarely shows up cleanly in an IT budget. Resolution time and ticket volume are tracked. The dollar value of every locked-out employee, every password reset, every identity check sits buried inside IT operating budgets that were never designed to surface it.

HDI benchmarks the average IT helpdesk ticket at \$25 in labor and tooling. Enterprise-grade identity verification cuts that by roughly 86%, primarily by routing the majority of verification events through self-service workflows that never touch the helpdesk.

MANUAL HELPDESK VERIFICATION



HDI benchmark — labor and tooling per ticket

ENTERPRISE IDV VERIFICATION



Nametag deployment data — about 14% of the \$25 baseline

| Routing the majority of events to self-service is what closes the gap.

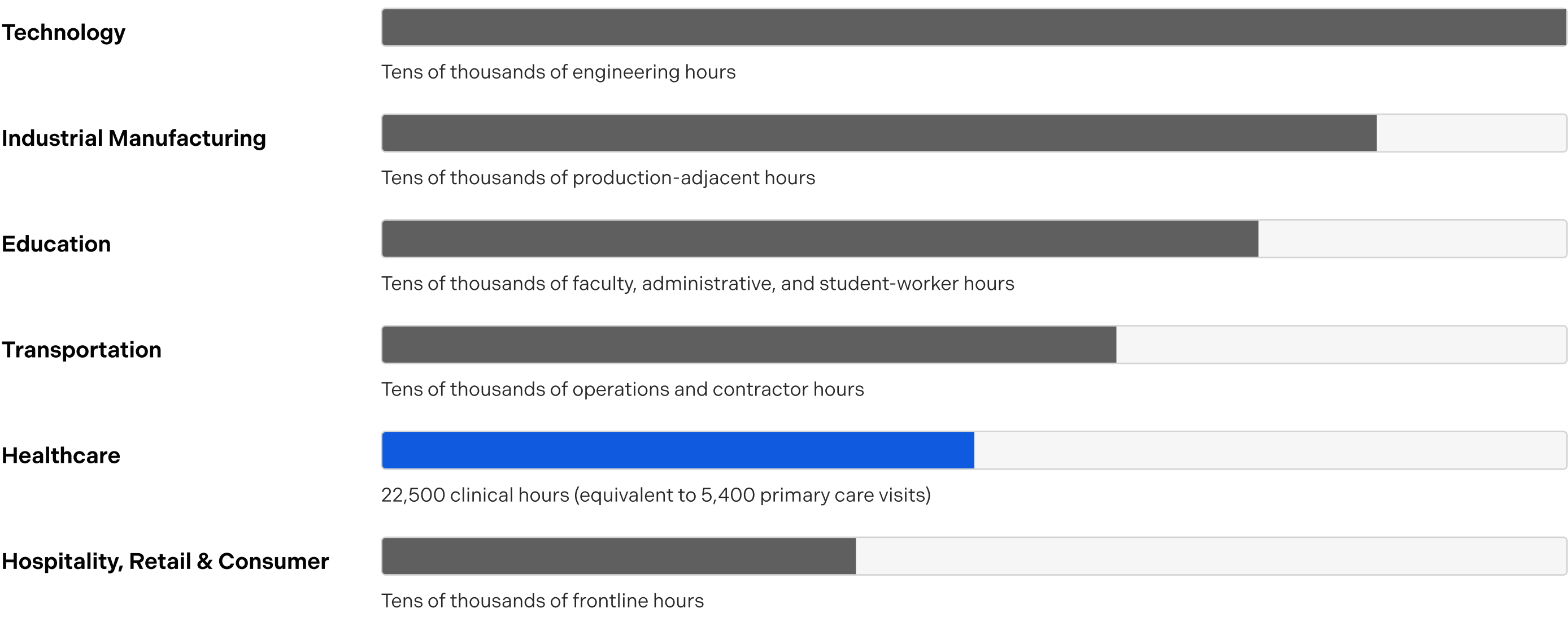
The per-ticket cost is just the surface. The hidden costs are where the real spend lives. Senior IAM engineers spend meaningful time patching custom verification logic and HRIS webhooks instead of building strategic capabilities. Custom integration work runs into tens of thousands of dollars per use case, with annual maintenance adding another 20% on top. Case escalations consume manager and HR time that does not appear on any IT report. And helpdesk headcount scales linearly with the workforce. Every new employee adds verification volume that has to be absorbed somewhere. Enterprise IDV breaks the linear scaling pattern. The IT organization can stop absorbing identity work as a growth tax.

Workforce Productivity

Every hour the helpdesk spends on identity verification is also an hour an employee spends waiting. Every escalation absorbed by a manager is salaried management time pulled away from the work the business is actually paying for. The same friction that shows up as a per-ticket cost on the IT side shows up as a productivity drain on the business side — and the business side is bigger.

For a 15,000-employee organization, the cumulative hours lost to identity friction — wait time on resets, verification queues, escalation handling, and the day-to-day drag of a process that asks the user to prove who they are without giving them a fast way to do it — easily run into the tens of thousands annually. Enterprise IDV cuts that volume by roughly 80%.

The chart shows hours of workforce capacity lost to identity friction across the six industry chapters, ranked by magnitude.



Hours are recovered when enterprise IDV replaces manual verification. The dollar value of those hours varies by sector, from \$1.92M in Hospitality, Retail & Consumer to \$4.48M in Technology. Bars follow the source ranking by magnitude; only the Healthcare figure is stated numerically in the source.

The hours themselves are not the cost. The cost is what those hours are worth. The fully loaded value of an employee hour ranges from roughly \$37 in hospitality and retail to nearly \$90 in technology. Multiply that by tens of thousands of recovered hours and the productivity cost recaptured runs into the millions — anywhere from \$1.9M in lower-wage industries to more than \$4.5M in higher-wage ones.

INDUSTRY	FULLY LOADED HOURLY RATE	ANNUAL PRODUCTIVITY LOSS	RECOVERED WITH ENTERPRISE IDV
Technology	~\$89/hr	\$4.48M	\$3.58M
Healthcare	~\$77/hr	\$1.86M	\$1.49M
Industrial Manufacturing	~\$54/hr	\$2.97M	\$2.38M
Education	~\$53/hr	\$2.97M	\$2.38M
Transportation	~\$50/hr	\$2.74M	\$2.19M
Hospitality, Retail & Consumer	~\$37/hr	\$1.92M	\$1.54M

The wait time is the obvious cost. Two less obvious patterns sit inside it.

The first is day-one onboarding. A new hire who cannot access core systems on their first day is a productivity loss the business has already paid for. For a 15,000-employee enterprise onboarding roughly 525 new hires annually, even modest onboarding delays compound. Salaries are paid against ramp time. Training resources are reserved. Manager attention is allocated. The cumulative cost runs into the millions.

The second is manager drag. A meaningful share of helpdesk tickets pull a manager into the resolution loop – vouching for the employee, approving an exception, sitting on a video call to confirm identity.

The Day-One Tax

Every new hire who cannot access core systems from their first hour of employment is a productivity loss the business has already paid for.

A verified human layer at the pre-hire and onboarding stage confirms identity at offer acceptance. Day 1 access is provisioned against a verified identity record. The first hour of employment becomes the first hour of contribution.

Identity friction looks like an IT cost on paper. The math says otherwise. It is a productivity tax paid by the business – billed quietly, in salaried hours, to every employee waiting on a verification the system should already trust.

Annual Loss Expectancy

Operational efficiency and workforce productivity are paid every day, in tickets and hours. They are real, but they are recoverable. Annual Loss Expectancy is different. It is the financial exposure that converts to a realized cost the moment an identity-based breach succeeds. The breach dynamics in 2026 make that moment more probable, more frequent, and more expensive than most organizations have priced in.

ALE is a standard actuarial calculation: the probability of a breach in a given year (Annual Rate of Occurrence) multiplied by the average cost of that breach when it happens (Single Loss Expectancy). Both inputs have moved against the enterprise over the past three years. Identity-based breach probability has risen as credentials became commodity, MFA aged, and AI lowered the cost of impersonation. Single Loss Expectancy has risen because the breaches that succeed reach further, dwell longer, and trigger heavier regulatory exposure than they did even a year ago.

IBM's 2025 Cost of a Data Breach Report puts the U.S. average at \$10.22M, a figure driven by the regulatory, litigation, and recovery cost structure unique to the U.S. market. The global average is \$4.4M. Healthcare leads every other sector at \$7.42M for the fourteenth consecutive year. Identity-driven breaches in Healthcare take longer to detect, longer to contain, and trigger broader compliance fallout when they involve credentialed access to sensitive systems.

The most useful way to think about ALE is not as an annual figure, but as a weekly one. Every week the gap stays open is a week of accumulated exposure that converts to realized cost the moment a successful breach occurs. For a healthcare organization, that ALE meter alone runs at roughly \$96,000 a week. For a technology firm, \$48,000. For a manufacturer, \$46,000. Layered with operational, productivity, and hiring fraud costs, the full weekly figure is meaningfully higher. The annual ALE is the headline. The weekly rate is what makes the cost of waiting feel like what it actually is.

STAGE	POSTURE	CHARACTERISTICS	RESIDUAL ALE
Stage 1	Manual Verification	Human judgment, no automation. Help desk staff verify identity using their best discretion.	Full baseline ALE — no reduction.
Stage 2	Compliance-Grade Verification	Point-in-time selfie matching, custom integration logic, developer maintenance burden.	50–60% of baseline ALE retained.
Stage 3	Security-Optimized Verification	3D liveness, cryptographic device binding, identity orchestration, expert-managed appeals, identity-to-enterprise account matching.	15–25% of baseline ALE retained.
Stage 4	Managed Enterprise Verification	Continuous assurance across the workforce lifecycle. Vendor-managed edge cases. Defensible audit posture.	Single digits as a percentage of baseline ALE.

The maturity of the identity verification posture maps directly to residual exposure. Manual verification carries the full ALE. Compliance-grade verification, with point-in-time selfie matching and custom integration logic, is estimated to reduce residual exposure to roughly 50 to 60% of baseline. Security-optimized verification — 3D liveness, cryptographic device binding, identity orchestration, expert-managed appeals, and identity-to-enterprise account matching — reduces residual exposure to roughly 15 to 25% of baseline. Managed enterprise verification, the Stage 4 posture, reduces residual exposure to single digits and converts each cost dimension from a recurring expense into a recovered margin.

Compliance-grade IDV is not a sufficient substitute. It clears the audit checkbox without closing the actuarial gap, and it carries hidden integration and maintenance costs that erode the headline savings.

INDUSTRY	AVERAGE BREACH COST	ANNUAL RATE OF OCCURRENCE	BASELINE ALE	RESIDUAL ALE WITH ENTERPRISE IDV
Healthcare	\$7.42M	67%	\$4.97M	\$397K
Technology	\$4.79M	52%	\$2.49M	\$199K
Industrial Manufacturing	\$5.00M	48%	\$2.40M	\$192K
Education	\$3.80M	58%	\$2.20M	\$176K
Hospitality, Retail & Consumer	\$4.03M	50%	\$2.02M	\$161K
Transportation	\$3.98M	32%	\$1.27M	\$121K

Every industry carries this exposure differently. Healthcare carries the highest ALE because identity-driven breaches in clinical environments trigger the longest dwell times and the broadest regulatory fallout. Technology carries it because a single compromised admin credential can propagate across an entire customer base before detection. Manufacturing carries it because a breach that reaches operational systems stops production, not just data. Hospitality, Retail & Consumer carries it because high-turnover environments produce the credential surface attackers exploit most frequently. The numbers vary, but the exposure is universal.

The Meter Is Running

Every week the workforce identity gap stays open is a week of accumulated exposure carried on the books. The annual ALE is the headline. The weekly rate is what makes the cost of waiting feel like what it actually is.

Healthcare	~\$96,000/week
Technology	~\$48,000/week
Industrial Manufacturing	~\$46,000/week
Education	~\$42,000/week
Hospitality, Retail & Consumer	~\$39,000/week
Transportation	~\$25,000/week

Weekly figures derived from baseline ALE divided across 52 weeks. The full weekly cost of doing nothing including operational, productivity, and hiring fraud. It is meaningfully higher per industry. See each chapter for the full picture.

Every week the gap stays open is a week of accumulated exposure that converts to realized cost the moment a successful breach occurs. For a healthcare organization, that meter runs at roughly \$96,000 a week. For a technology firm, \$48,000. For a manufacturer, \$46,000. The annual ALE is the headline. The weekly rate is what makes the cost of waiting feel like what it actually is.

Hiring Fraud

Hiring fraud is the identity risk that arrives before the employee's first day. The fraud rate has climbed sharply over the past three years. The legal exposure attached to it has climbed faster.

A Gartner survey found candidate fraud makes up roughly 25% of application volume in remote technology roles in 2026. Most of that comes from automated AI-generated applications and resume fraud. A smaller and far more dangerous fraction comes from sophisticated identity impersonation. Mandiant's M-Trends 2026 report documents that North Korean IT worker operations remained a persistent insider threat throughout 2025, with a median dwell time of 122 days before detection and some cases persisting undetected for over a year.

The U.S. Treasury, FBI, and DOJ have been explicit about the threat. State-sponsored operatives, primarily from North Korea, are using AI-generated profiles, deepfake interview tooling, and U.S.-based laptop farms to embed themselves directly into Western corporate payrolls. The March 2026 OFAC sanctions action named individuals and entities tied to operations that have generated hundreds of millions of dollars in revenue for the regime. A single 2025 federal case named 309 U.S. companies that had unknowingly placed North Korean operatives on payroll, including Fortune 500 companies in technology, aerospace, automotive, and media.

The cost shows up in three places.

1.Application Authenticity

The first place cost shows up is in the labor an enterprise spends investigating suspect applicants; cross-referencing profiles, verifying employer history, validating headshots. At typical enterprise hiring volumes, that investigative work runs to roughly 2,600 recruiter hours per year. At a fully loaded recruiter rate of \$43 per hour, the annual cost is roughly \$112,000 in labor the organization absorbs whether or not it catches a fraudulent hire.

2.Fraudulent hire economics

Next is the cost of the infiltrations that succeed. A fraudulent hire draws a salary against the 122-day median dwell time before detection, runs through a ramp period where productivity is effectively zero, and leaves a vacancy that has to be backfilled. For a typical enterprise, that produces roughly eight fraudulent placements per year. Salary paid runs to roughly \$625,000. Productivity loss across ramp and vacancy adds another \$415,000. Total annual cost: roughly \$1.08M.

3.OFAC Sanctions Exposure

The last place is categorical. Civil penalties for paying a sanctioned individual are strict liability under federal law. Intent does not matter. Awareness does not matter. The penalty runs at up to \$377,000 per paycheck issued, and every paycheck issued to a sanctioned worker is treated as a separate violation. A single fraudulent placement over the 122-day median dwell generates roughly nine paychecks before detection. That is a maximum exposure of \$26.7M per event, before any criminal exposure or remediation cost is added.

Application Authenticity Recruiter labor investigating suspect applicants. ~2,600 hours annually at \$43/hr fully loaded. \$112K Annual cost	Fraudulent Hire Economics Salary paid against 122-day median dwell, ramp loss, vacancy cost. ~8 fraudulent placements per year at typical enterprise. \$1.08M Annual cost	OFAC Sanctions Exposure \$377K civil penalty per paycheck issued to a sanctioned worker. 9 paychecks against the 122-day median dwell time. \$26.7M Maximum exposure, per placement
---	--	--

Buckets 1 and 2 are operational costs that scale with hiring volume. Bucket 3 is a categorical exposure under strict liability federal law.

OFAC: Strict Liability by Design

Civil penalties under federal sanctions law do not require intent. They do not require awareness. They do not require evidence that the employer knew the worker was sanctioned.

They require only that a paycheck was issued.

Maximum penalty per paycheck issued	\$377,000
Each paycheck treated as a separate violation	—
122-day median dwell time	≈ nine paychecks
Maximum civil exposure per placement	\$26.7M

Background checks do not catch this. They confirm that records match, not that the person presenting them is real. State-sponsored operatives use stolen identities from actual U.S. citizens whose records pass every standard check cleanly.

CHECK	WHAT IT CONFIRMS	WHAT IT MISSES
Background check	Records match the candidate's stated history	Whether the person presenting the records is real
Reference check	Stated employment history is plausible	Whether the candidate is the person who held the prior roles
Video interview	A face matches the documents	Whether the face on camera is the face that shows up Day one
Document verification	Documents are formatted correctly	Whether documents belong to the person submitting them
Workforce identity verification	The human matches the credentials and the work history	—

The operational cost of hiring fraud runs to roughly \$1.19M annually for a typical enterprise — investigation labor plus the fraudulent hires that slip through. OFAC sanctions liability sits on top of that as a regulator-driven exposure that does not require a successful breach to land. It requires only that one fraudulent applicant make it through a verification process that was never designed to catch them.

Operational efficiency, workforce productivity, actuarial exposure, and sanctions liability. The bill is already running. The amount each enterprise pays varies by industry. The next section quantifies what it looks like by sector.

What Doing Nothing Costs By Industry

The four cost dimensions apply to every enterprise. The financial weight of each one does not.

A recovered hour in Healthcare is worth nearly two and a half times a recovered hour in Retail. The Annual Loss Expectancy in Healthcare is roughly double the figure in Technology. The hiring fraud exposure in Technology is categorically different from the exposure in Manufacturing. Industry shapes which dimension dominates, how fast the cost compounds, and what closing the gap returns first.

Operational Efficiency The IT labor and overhead burden of manual identity verification. \$1.25M Baseline → \$172K with enterprise IDV 86% reduction	Workforce Productivity Varies by sector with fully loaded compensation. \$1.92M – \$4.48M Hospitality (low) → Technology (high)	Annual Loss Expectancy Varies by sector with breach probability and cost. \$1.27M – \$4.97M Transportation (low) → Healthcare (high)	Hiring Fraud Varies by sector, plus categorical OFAC liability. \$699K – \$1.99M Hospitality (low) → Technology (high) up to \$26.7M OFAC, per placement
---	---	--	---

Operational efficiency is roughly constant across sectors at this workforce size; the other three dimensions scale with sector economics. OFAC sanctions liability sits on top as a categorical exposure not included in the totals below.

INDUSTRY	TOTAL ANNUAL COST	WEEKLY INACTION RATE
Healthcare	\$7.8M	\$150,000/week
Technology	\$6.96M	\$134,000/week
Industrial Manufacturing	\$6.54M	\$126,000/week
Education	\$5.25M	\$101,000/week
Transportation	\$4.31M	\$83,000/week
Hospitality, Retail & Consumer	\$4.12M	\$79,000/week

Figures are illustrative for a 15,000-employee organization. OFAC sanctions liability sits on top as a categorical exposure not included in the totals above.

Take a deeper look into six industries where the gap is widest and the cost is most immediate: Healthcare; Technology; Hospitality, Retail & Consumer; Industrial Manufacturing; Education; and Transportation.

Jump to industry

Healthcare

Technology

Hospitality, Retail & Consumer

Industrial Manufacturing

Education

Transportation

Healthcare

Healthcare runs on identity at a scale no other sector matches. A typical physician carries dozens of active logins across the EMR, scheduling, e-prescribing, imaging, and affiliate systems. The workforce runs 24/7 in rotational shifts. Affiliate clinicians, locum tenens, and contracted specialists move through the same identity stack as employees, with materially weaker governance. Sprawl multiplies the recovery events. Rotation spreads them across hours when the helpdesk is not fully staffed. Affiliate access widens the population presenting them.

Change Healthcare

The breach did not begin with a software exploit. It began with credentials on a Citrix portal that had no multi-factor authentication. Once inside, attackers operated for nine days before deploying ransomware. The incident disrupted pharmacy operations, claims processing, and clinical workflows across the U.S. healthcare system for weeks. UnitedHealth Group reported the financial impact at \$872M in the first quarter following the attack.

The cost shows up across four dimensions, and Healthcare carries the highest exposure of any sector in three of them.

Workforce Productivity

A 15,000-employee health system loses roughly 22,500 clinical hours each year to the verification queue. That is the equivalent of 5,400 primary care visits the system already scheduled, staffed, and lost to identity friction. The patients still need care; the institution still pays for it; the hours just do not come back. Enterprise IDV is estimated to recover 80% of those hours and return roughly 18,000 of them to the floor.

Annual Loss Expectancy

Healthcare's Annual Loss Expectancy from identity-driven breaches sits at \$4.97M baseline — higher than any other sector. IBM's 2025 Cost of a Data Breach Report puts Healthcare at \$7.42M average breach cost, leading every other sector for the fourteenth consecutive year. The breaches that involve credentialed access to patient data take longer to detect, longer to contain, and trigger broader compliance fallout than breaches anywhere else. Enterprise IDV is estimated to reduce that exposure to \$397K, a 92% reduction. The \$4.57M actuarial gap is carried on the books whether the breach happens or not.

Operational Efficiency

Identity-related ticket volume at a 15,000-employee health system runs to roughly \$1.25M in IT labor each year at a \$25 manual baseline. Enterprise IDV cuts per-ticket cost to \$3.45 — an 86% reduction when compared to manual verification processes — and recovers roughly \$1.08M annually in operational capacity that has historically been spent on credential resets and verification calls.

Hiring Fraud

Healthcare absorbs roughly \$1.24M each year across the three hiring fraud cost buckets: the recruiter labor that investigates suspect applicants, the salary paid against the 122-day median dwell time of a fraudulent placement, and the ramp and vacancy loss of bad hires who slip through. OFAC sanctions liability sits on top as a categorical exposure — up to \$26.7M per fraudulent placement, with strict liability under federal law.

Workforce Productivity 22,500 clinical hours lost annually, equivalent to 5,400 primary care visits. \$1.86M In productivity cost	Annual Loss Expectancy The highest actuarial gap of any sector. \$4.97M Baseline ALE → \$397K with enterprise IDV \$4.57M actuarial gap, highest of any sector	Operational Efficiency Manual ticket labor versus enterprise IDV. \$1.25M In IT labor at manual baseline \$1.08M recovered with enterprise IDV 86% reduction in per-ticket cost	Hiring Fraud Recruiter labor, fraudulent-hire economics, ramp and vacancy loss. \$1.24M Annual operational cost Up to \$26.7M per OFAC violation — strict liability
TOTAL ANNUAL COST OF DOING NOTHING \$7.8M		WEEKLY INACTION RATE \$150,000/week	

Figures are illustrative for a 15,000-employee health system. OFAC liability is not included in the total.

Stacked together, the cost of doing nothing in Healthcare runs to roughly \$7.8M annually for a 15,000-employee health system before OFAC liability is layered on. The figure runs by the week. Every seven days the gap stays open is roughly \$150,000 of accumulated exposure that converts to realized cost the moment a successful breach occurs.

The math runs the other direction once the gap closes. A single verified human layer resolves the recovery flow, the EMR access point, the affiliate provisioning workflow, and the high-privilege approval. The result is patient access returned to the floor, defensible audit posture across every credentialed system, and IT spend that stops growing on a curve the budget cannot absorb.

CFO \$4.57M annual ALE reduction Total recovered: \$6.5M annually. License cost lands at roughly 2% of manual TCO.	CISO 92% reduction in Annual Rate of Occurrence Audit-defensible verification at every EMR access point, affiliate credential issuance, and high-risk hire.	CIO IT headcount stays flat as the rotational workforce scales Self-service absorbs the 3am credential reset volume that has historically driven helpdesk growth.
---	--	--

Each outcome is produced by the same control, deployed once.

For Healthcare, the cost of doing nothing is not abstract. It is paid in hours that should have gone to patients, in audit findings that surface every time PHI is touched by an unverified user, in helpdesk capacity consumed by credential resets, and in hiring decisions that no background check was designed to verify. Each cost compounds with the next. Closing the gap once returns clinical hours, audit defensibility, IT capacity, and hire confidence simultaneously.

Technology

Technology runs on engineering velocity. Every hour an engineer spends on credential resets, MFA recovery, or admin credential reissuance is an hour the roadmap does not move. The cost is concentrated in the most expensive labor in the company.

A 15,000-employee technology firm loses tens of thousands of engineering hours each year to identity friction. The structural conditions are specific to the sector: DevOps and admin users carry production-level access that traditional verification cannot keep pace with under agile deployment cycles. Synthetic identities and deepfake-enabled interview tooling are an active and validated 2026 threat against engineering hiring. A single compromised credential at a SaaS provider propagates across the customer base.

Snowflake

The breach did not begin with a software exploit. It began with credential stuffing against customer accounts that lacked multi-factor authentication. Once inside, attackers exfiltrated data from more than 160 enterprise customers, demonstrating that the provider's identity posture becomes every customer's risk.

The cost shows up across four dimensions, and Technology carries the highest exposure of any sector in two of them.

Workforce Productivity

Workforce productivity loss in Technology runs to \$4.48M annually — the highest of any sector in this report — concentrated in engineering, where the highest-paid talent in the company spends time on resets and reissuance instead of shipping. Enterprise IDV is estimated to recover 80% of those hours and return roughly \$3.58M annually in engineering capacity to the roadmap.

Annual Loss Expectancy

Technology's Annual Loss Expectancy from identity-driven breaches sits at \$2.49M baseline. Identity-driven breaches in Technology take longer to surface than in any other sector — the average dwell time is 210 days — because the same DevOps access pattern that enables velocity also makes anomalous behavior harder to distinguish from legitimate activity. Enterprise IDV is estimated to reduce that exposure to \$199K, a 92% reduction.

Operational Efficiency

Identity-related ticket volume at a 15,000-employee technology firm runs to \$1.25M in IT labor annually at a \$25 manual baseline. Enterprise IDV cuts per-ticket cost to \$3.45 — an 86% reduction when compared to manual verification processes — and recovers roughly \$1.08M annually in operational capacity.

Hiring Fraud

Technology absorbs roughly \$1.99M each year — the highest hiring fraud cost of any sector in this report — across the three hiring fraud cost buckets. The driver is specific: state-sponsored operatives target technology roles because remote engineering hiring is the entry point most accessible to deepfake-enabled impersonation. OFAC sanctions liability sits on top as a categorical exposure — up to \$26.7M per fraudulent placement, with strict liability under federal law.

Workforce Productivity Concentrated in engineering hours absorbed by credential resets — the highest of any sector. \$4.48M Productivity loss annually \$3.58M recovered with enterprise IDV	Annual Loss Expectancy 210-day average dwell time before detection — the longest of any sector. \$2.49M Baseline ALE → \$199K with enterprise IDV	Operational Efficiency Manual ticket labor versus enterprise IDV. \$1.25M In IT labor at manual baseline \$1.08M recovered with enterprise IDV 86% reduction in per-ticket cost	Hiring Fraud The highest hiring fraud cost of any sector in this report. \$1.99M Annual operational cost Up to \$26.7M per OFAC violation
TOTAL ANNUAL COST OF DOING NOTHING \$6.96M		WEEKLY INACTION RATE \$134,000/week	

Figures are illustrative for a 15,000-employee technology firm. OFAC liability is not included in the total.

Stacked together, the cost of doing nothing in Technology runs to roughly \$6.96M annually for a 15,000-employee firm before OFAC liability is layered on. The figure runs by the week. Every seven days the gap stays open is roughly \$134,000 of accumulated exposure that converts to realized cost the moment a successful breach occurs.

The math runs the other direction once the gap closes. A single verified human layer resolves the recovery flow, the DevOps high-privilege approval, the engineering onboarding workflow, and the admin credential issuance. The result is engineering capacity returned to the roadmap, dwell time compressed from months to days, and a hiring pipeline that filters synthetic identities before they reach payroll.

CFO \$2.29M annual ALE reduction Total recovered: \$5.8M annually. License cost lands at roughly 2% of manual TCO.	CISO 92% reduction in Annual Rate of Occurrence Dwell time compressed from months to days. Audit-defensible verification at every DevOps high-privilege approval and admin credential issuance.	CIO IT headcount stays flat as the engineering organization scales Self-service absorbs the lockout and reset volume that has historically pulled engineers off the work.
--	---	---

Each outcome is produced by the same control, deployed once.

For Technology, the cost of doing nothing is paid in the same currency the business runs on. Engineering hours absorbed by credential resets instead of code. Admin credentials that compromise entire customer bases when they are taken. Helpdesk capacity that grows with every new hire. Hiring decisions that no remote interview was designed to verify. Each cost compounds with the next. Closing the

Hospitality, Retail & Consumer

For Hospitality, Retail & Consumer, the helpdesk is the entry point of choice. Attackers know it. The most consequential identity breaches of the past three years in this sector began with a phone call to the helpdesk, a voice impersonating a store manager or shift supervisor, and a credential reset processed under the urgency that defines retail and hospitality operations. The cost of getting that verification call wrong scales with the value of what the breached account can touch.

A typical organization in this sector runs a workforce with 70 to 100% annual turnover on the frontline. The identity governance gap is perpetual rather than periodic. Offboarding failures at this scale are not edge cases; they are structural. The helpdesk absorbs the volume of credential resets, MFA recoveries, and new-hire enrollments that scale with that turnover, and verification rigor degrades under the pressure.

MGM Resorts and Caesars Entertainment

The breach did not begin with a software exploit. It began with a ten-minute social engineering call to the helpdesk. Once attackers had the credentials they needed, hotel and casino operations were shut down for days, and the financial impact ran into the hundreds of millions of dollars.

The cost shows up across four dimensions.

Annual Loss Expectancy

Hospitality, Retail & Consumer carries an Annual Loss Expectancy of \$2.02M baseline. IBM's 2025 Cost of a Data Breach Report puts the sector at \$4.03M average breach cost. The breaches that succeed in this sector tend to land deep — store systems, payment infrastructure, customer data, and operational technology — because the workforce identities attackers compromise often hold access to systems that span every layer of the business. Enterprise IDV is estimated to reduce that exposure to \$161K, a 92% reduction.

Marks & Spencer

The breach did not begin with a software exploit. It began with compromised identity. Once inside, attackers used trusted accounts and existing permissions to operate in plain sight, and the disruption extended across the retail operation.

Workforce Productivity

Workforce productivity loss in Hospitality, Retail & Consumer runs to \$1.92M annually. The cost is distributed across frontline staff at thousands of locations, where credential reset delays mean a shift cannot start, a register cannot open, or a guest cannot be served. Enterprise IDV is estimated to recover 80% of those hours and return roughly \$1.54M annually in operational capacity to the floor.

Operational Efficiency

Identity-related ticket volume at a 15,000-employee organization in this sector runs to \$1.25M in IT labor annually at a \$25 manual baseline. Enterprise IDV cuts per-ticket cost to \$3.45 — an 86% reduction when compared to manual verification processes — and recovers roughly \$1.08M annually in operational capacity.

Hiring Fraud

Hospitality, Retail & Consumer absorbs roughly \$699K each year across the three hiring fraud cost buckets. The sector sits at the lower end of the cross-industry range for hiring fraud exposure, primarily because the median frontline role is less attractive to state-sponsored placement than engineering, financial services, or aerospace roles. OFAC sanctions liability still sits on top as a categorical exposure — up to \$26.7M per fraudulent placement, with strict liability under federal law.

Annual Loss Expectancy	Workforce Productivity	Operational Efficiency	Hiring Fraud
Breaches land deep — store systems, payment, customer data, and OT.	Cost distributed across thousands of frontline locations.	Manual ticket labor versus enterprise IDV.	Lower end of the cross-industry range.
\$2.02M	\$1.92M	\$1.25M	\$699K
Baseline ALE → \$161K with enterprise IDV	Productivity loss annually	In IT labor at manual baseline	Annual operational cost
92% reduction	\$1.54M recovered with enterprise IDV	\$1.08M recovered with enterprise IDV	Up to \$26.7M per OFAC violation
		86% reduction in per-ticket cost	
TOTAL ANNUAL COST OF DOING NOTHING		WEEKLY INACTION RATE	
\$4.12M		\$79,000/week	

Figures are illustrative for a 15,000-employee organization. OFAC liability is not included in the total.

Stacked together, the cost of doing nothing in Hospitality, Retail & Consumer runs to roughly \$4.12M annually for a 15,000-employee organization before OFAC liability is layered on. The figure runs by the week. Every seven days the gap stays open is roughly \$79,000 of accumulated exposure that converts to realized cost the moment a successful breach occurs.

The math runs the other direction once the gap closes. A single verified human layer resolves the recovery flow, the helpdesk verification call, the seasonal onboarding workflow, and the high-privilege approval. The result is a helpdesk that stops functioning as the attack surface, frontline capacity returned to the floor, and an identity posture that is consistent across thousands of distributed locations without scaling helpdesk headcount.

CFO \$1.85M annual ALE reduction Total recovered: \$3.5M annually. License cost lands at roughly 2% of manual TCO.	CISO 92% reduction in Annual Rate of Occurrence Audit-defensible verification at every helpdesk recovery flow and seasonal onboarding event. Closes the entry point attackers most commonly use against the sector.	CIO IT headcount stays flat as the seasonal and frontline workforce scales Self-service absorbs the verification volume that historically saturated the helpdesk and exposed it to social engineering.
--	---	--

Each outcome is produced by the same control, deployed once.

For Hospitality, Retail & Consumer, the cost of doing nothing is paid at the front door of every identity event. In the helpdesk call that lets an attacker in. In the credential reset that happens faster than verification can keep up. In the frontline workforce that turns over faster than offboarding can catch. In the hires that come through high-volume channels that no background check was designed to verify. Each cost compounds with the next. Closing the gap once turns the helpdesk from an attack surface back into a service function.

Skip remaining industries

Industrial Manufacturing

For Industrial Manufacturing, a breach in operational systems does not just compromise data. It stops production. The cost of identity friction in this sector scales with throughput — every hour of operational downtime carries a cost no other sector pays, and a breach that reaches the line does damage that data-only sectors are spared.

A typical 15,000-employee manufacturer runs a mixed workforce: employees, contractors, third-party engineers, shift workers, and field technicians move through the same identity stack with different governance. Shift schedules do not align with centralized helpdesk hours. OT and IT systems that were once isolated are increasingly converged, which means workforce identities now touch production systems they previously did not. Each of those structural conditions widens the surface attackers exploit.

Jaguar Land Rover

The breach did not begin with a software exploit. It began with compromised identity. Attackers used trusted accounts and existing permissions to operate in plain sight, and the recovery extended well beyond the IT environment.

The cost shows up across four dimensions, and Industrial Manufacturing carries the second-highest workforce productivity exposure of any sector in this report.

Annual Loss Expectancy

Industrial Manufacturing carries an Annual Loss Expectancy of \$2.4M baseline. IBM's 2025 Cost of a Data Breach Report puts Manufacturing at \$5.0M average breach cost — the second-highest of any sector, behind only Healthcare. Identity-driven breaches that reach operational systems trigger production disruption that ripples through the supply chain, vendor relationships, and customer commitments. Enterprise IDV is estimated to reduce that exposure to \$192K, a 92% reduction.

Workforce Productivity

Workforce productivity loss in Industrial Manufacturing runs to \$2.97M annually — the second-highest of any sector after Technology. The cost is concentrated where production cannot wait: shift handoffs that stall on credential resets, line restarts delayed by MFA recovery, supplier and contractor credential issuance that holds up coordinated work. Enterprise IDV is estimated to recover 80% of those hours and return roughly \$2.38M annually in operational capacity.

Operational Efficiency

Identity-related ticket volume at a 15,000-employee manufacturer runs to \$1.25M in IT labor annually at a \$25 manual baseline. Enterprise IDV cuts per-ticket cost to \$3.45 — an 86% reduction when compared to manual verification processes — and recovers roughly \$1.08M annually in operational capacity.

Hiring Fraud

Industrial Manufacturing absorbs roughly \$1.19M each year across the three hiring fraud cost buckets. The sector is exposed to state-sponsored placement because of the concentration of intellectual property, defense-adjacent supply chains, and proprietary process knowledge in the workforce. OFAC sanctions liability sits on top as a categorical exposure — up to \$26.7M per fraudulent placement, with strict liability under federal law.

Annual Loss Expectancy \$5.0M average breach cost — second-highest of any sector. \$2.4M Baseline ALE → \$192K with enterprise IDV	Workforce Productivity The second-highest of any sector, after Technology. \$2.97M Productivity loss annually \$2.38M recovered with enterprise IDV	Operational Efficiency Manual ticket labor versus enterprise IDV. \$1.25M In IT labor at manual baseline \$1.08M recovered with enterprise IDV 86% reduction in per-ticket cost	Hiring Fraud Exposure concentrated in IP-rich and defense-adjacent roles. \$1.19M Annual operational cost Up to \$26.7M per OFAC violation
TOTAL ANNUAL COST OF DOING NOTHING \$6.54M		WEEKLY INACTION RATE \$126,000/week	

Figures are illustrative for a 15,000-employee manufacturer. OFAC liability is not included in the total.

Stacked together, the cost of doing nothing in Industrial Manufacturing runs to roughly \$6.54M annually for a 15,000-employee manufacturer before OFAC liability is layered on. The figure runs by the week. Every seven days the gap stays open is roughly \$126,000 of accumulated exposure that converts to realized cost the moment a successful breach occurs.

The math runs the other direction once the gap closes. A single verified human layer resolves the recovery flow, the OT system access point, the contractor credential issuance, and the high-privilege approval. The result is production lines that do not stop on a credential reset, contractor and supplier access provisioned with audit-defensible verification, and operational capacity returned across every shift the workforce runs.

CFO \$2.21M annual ALE reduction Total recovered: \$5.4M annually. License cost lands at roughly 2% of manual TCO.	CISO 92% reduction in Annual Rate of Occurrence Audit-defensible verification at every OT system access point and contractor credential issuance.	CIO IT headcount stays flat as the mixed contractor workforce scales Self-service absorbs the credential reset volume that has historically pulled IT support off operational priorities.
---	--	--

Each outcome is produced by the same control, deployed once.

For Industrial Manufacturing, identity friction is paid where the business actually runs. In the shift that cannot start because the helpdesk has not opened. In the OT system that a compromised identity now reaches. In the contractor whose credentials carry consequences they were never scoped for. In the hiring pipeline that lets a state-sponsored operative onto a factory floor with access to proprietary process knowledge. Each cost compounds with the next. Closing the gap once returns the production line, the contractor credential, the

Education

For Education, the workforce is not a workforce. It is multiple workforces operating on the same identity stack with materially different access patterns and governance. Faculty hold the keys to intellectual property and grant administration. Administrative staff manage financial aid, student PII, payroll, and vendor payments. Student workers and graduate assistants access institutional systems from personal devices with limited security training. Affiliates, visiting researchers, and contracted clinicians at academic medical centers move through the same identity flows as employees but with weaker offboarding rigor.

A typical 15,000-employee educational institution operates this identity model under structural pressure that few other sectors face. The U.S. Department of Education reports that school districts face an average of five cyber incidents per week, disrupting teaching, payroll, vendor payments, and day-to-day school operations. The institutional data Education holds — high-quality PII paired with financial records, including student loan information — is among the most targeted in the threat landscape for synthetic identity theft. And the supply chain Education depends on (learning management systems, ERP platforms, scholarship and financial aid administration) widens the identity attack surface beyond the institution's own perimeter.

Canvas / Instructure

The breach did not begin with a software exploit. It began with the identity surface Canvas presents to its educational customers. ShinyHunters exfiltrated user data tied to roughly 8,800 schools, universities, and online education platforms, demonstrating that a single provider's identity posture becomes the risk of every institution it serves.

The cost shows up across four dimensions.

Annual Loss Expectancy

Education carries an Annual Loss Expectancy of \$2.20M baseline. IBM's 2025 Cost of a Data Breach Report puts Education at \$3.80M average breach cost. Identity-driven breaches in Education tend to cascade — a compromised student information system or LMS reaches every institution that depends on the provider, and the breach economics scale with the sprawl of the affected population. Enterprise IDV is estimated to reduce that exposure to \$176K, a 92% reduction.

Workforce Productivity

Workforce productivity loss in Education runs to \$2.97M annually. The cost is concentrated in faculty time absorbed by credential issues, administrative staff handling identity friction during financial aid disbursement and registration windows, and student workers waiting for access that helpdesks structured around 9-to-5 operations cannot reliably provide. Enterprise IDV is estimated to recover 80% of those hours and return roughly \$2.38M annually in institutional capacity.

Operational Efficiency

Identity-related ticket volume at a 15,000-employee educational institution runs to \$1.25M in IT labor annually at a \$25 manual baseline. Enterprise IDV cuts per-ticket cost to \$3.45 — an 86% reduction when compared to manual verification processes — and recovers roughly \$1.08M annually in operational capacity.

Hiring Fraud

Education absorbs roughly \$1.19M each year across the three hiring fraud cost buckets. The sector is exposed to candidate fraud across faculty, researcher, and administrative roles, particularly in research-intensive institutions where grant administration and IP access concentrate. OFAC sanctions liability sits on top as a categorical exposure — up to \$26.7M per fraudulent placement, with strict liability under federal law.

Annual Loss Expectancy \$3.80M average breach cost; breaches cascade across dependent institutions. \$2.20M Baseline ALE → \$176K with enterprise IDV 92% reduction	Workforce Productivity Concentrated in faculty hours and registration / financial aid windows. \$2.97M Productivity loss annually \$2.38M recovered with enterprise IDV	Operational Efficiency Manual ticket labor versus enterprise IDV. \$1.25M In IT labor at manual baseline \$1.08M recovered with enterprise IDV 86% reduction in per-ticket cost	Hiring Fraud Exposure concentrated in research-intensive faculty and grant administration roles. \$1.19M Annual operational cost Up to \$26.7M per OFAC violation
TOTAL ANNUAL COST OF DOING NOTHING \$5.25M		WEEKLY INACTION RATE \$101,000/week	

Figures are illustrative for a 15,000-employee educational institution. Supporting context: the U.S. Department of Education reports school districts face an average of five cyber incidents per week. OFAC liability is not included in the total.

Stacked together, the cost of doing nothing in Education runs to roughly \$5.25M annually for a 15,000-employee institution before OFAC liability is layered on. The figure runs by the week. Every seven days the gap stays open is roughly \$101,000 of accumulated exposure that converts to realized cost the moment a successful breach occurs.

The math runs the other direction once the gap closes. A single verified human layer resolves the recovery flow, the term-start access point, the affiliate provisioning workflow, and the high-privilege approval. The result is institutional continuity that holds across every workforce segment, financial aid and registration windows that proceed without identity friction, and an identity posture that protects the data students and families entrust to the institution.

CFO \$2.02M annual ALE reduction Total recovered: \$4.1M annually. License cost lands at roughly 2% of manual TCO.	CISO 92% reduction in Annual Rate of Occurrence Audit-defensible verification at every financial aid administration access point, faculty credential issuance, and supply-chain integration.	CIO IT headcount stays flat as the term-start and academic-year workforce scales Self-service absorbs the verification volume that decentralized helpdesks cannot.
--	--	--

Each outcome is produced by the same control, deployed once.

For Education, the cost of doing nothing is paid across every constituency the institution serves. In faculty hours pulled from research and teaching. In administrative staff time absorbed by verification calls during the windows when registration and financial aid cannot wait. In student worker access delays that compound across thousands of credentialed users. In the supply chain that delivers learning platforms, financial systems, and grant administration into institutional reach. Each cost compounds with the next. Closing the gap once protects every credentialed relationship the institution depends on.

Skip remaining industry

Transportation

For Transportation, an identity-driven breach does not stop at data. It diverts shipments, reroutes cargo, and triggers safety consequences that scale with throughput. The cost of identity friction in this sector is paid in physical disruption that other sectors do not face — every load that moves on a compromised credential is a load that has to be tracked, recovered, or written off.

A typical 15,000-employee transportation operator runs a workforce that is mobile, distributed, and partially external. Drivers, pilots, and maritime workers require secure remote access to manifests and navigation systems from environments where helpdesk support is hours away. Maintenance crews and gate agents work on shared kiosks and terminals where credential reuse is routine. Third-party mechanics, logistics partners, and contractors hold scoped temporary access through the same flows as full-time employees. The TSA's surface transportation directives require operators in the sector to designate a cyber coordinator, report incidents within fixed windows, maintain a response plan, and conduct regular vulnerability assessments. Identity verification is the foundation of every one of those requirements.

Diesel Vortex Cargo Theft Operation

The campaign did not begin with software exploits. It began with voice-AI impersonation used to steal credentials from freight brokers and carrier dispatchers. Once attackers held the workforce identity, they posted fraudulent load board listings, tricked legitimate shippers into releasing high-value cargo to complicit drivers, and rerouted goods for resale. The operation generated \$725M in cargo losses and demonstrated how a single compromised administrative identity can paralyze a supply chain.

The cost shows up across four dimensions.

Annual Loss Expectancy

Transportation carries an Annual Loss Expectancy of \$1.27M baseline — the lowest of any sector in this report. The figure understates the sector's true exposure because operational consequences are not fully captured in breach cost averages. A successful identity-based breach in Transportation reaches into cargo systems, load boards, dispatch operations, and yard access in ways that produce physical loss alongside data loss. Enterprise IDV is estimated to reduce that exposure to \$121K, a 90.5% reduction.

Workforce Productivity

Workforce productivity loss in Transportation runs to \$2.74M annually — the third-highest of any sector, after Technology and Manufacturing. The cost is concentrated where operations cannot wait: a driver at a yard gate waiting for a credential reset, a contractor on a tarmac who cannot access manifest systems, a maintenance crew whose start time depends on a helpdesk hours away. Enterprise IDV is estimated to recover 80% of those hours and return roughly \$2.19M annually in operational capacity.

Operational Efficiency

Identity-related ticket volume at a 15,000-employee transportation operator runs to \$1.25M in IT labor annually at a \$25 manual baseline. Enterprise IDV cuts per-ticket cost to \$3.45 — an 86% reduction when compared to manual verification processes — and recovers roughly \$1.08M annually in operational capacity.

Hiring Fraud

Transportation absorbs roughly \$1.49M each year across the three hiring fraud cost buckets – the fourth-highest of any sector in this report. The sector is exposed to candidate fraud particularly at the contractor and third-party engineer layer, where temporary access provisioning is the entry point most accessible to identity impersonation. Identity fraud in logistics is rising on its own track: approximately 3.2% of submitted credentials in logistics workflows are fraudulent or expired, and synthetic identities are increasingly used to divert shipments. OFAC sanctions liability sits on top as a categorical exposure – up to \$26.7M per fraudulent placement, with strict liability under federal law.

Annual Loss Expectancy	Workforce Productivity	Operational Efficiency	Hiring Fraud
Headline figure understates true exposure given physical consequences.	The third-highest of any sector, after Technology and Manufacturing.	Manual ticket labor versus enterprise IDV.	The fourth-highest of any sector; 3.2% of submitted logistics credentials are fraudulent or expired.
\$1.27M	\$2.74M	\$1.25M	\$1.49M
Baseline ALE → \$121K with enterprise IDV 90.5% reduction	Productivity loss annually \$2.19M recovered with enterprise IDV	In IT labor at manual baseline \$1.08M recovered with enterprise IDV 86% reduction in per-ticket cost	Annual operational cost Up to \$26.7M per OFAC violation
TOTAL ANNUAL COST OF DOING NOTHING		WEEKLY INACTION RATE	
\$4.31M		\$83,000/week	

Figures are illustrative for a 15,000-employee transportation operator. OFAC liability is not included in the total.

Stacked together, the cost of doing nothing in Transportation runs to roughly \$4.31M annually for a 15,000-employee operator before OFAC liability is layered on. The figure runs by the week. Every seven days the gap stays open is roughly \$83,000 of accumulated exposure that converts to realized cost the moment a successful breach occurs.

The math runs the other direction once the gap closes. A single verified human layer resolves the recovery flow, the remote operator access point, the contractor credential issuance, and the high-privilege approval. The result is fleet operations that do not pause for credential resets, contractor and supplier access provisioned with audit-defensible verification, and identity posture that satisfies the federal requirements TSA directives establish.

CFO \$1.15M annual ALE reduction Total recovered: \$3.3M annually. License cost lands at roughly 2% of manual TCO.	CISO 90.5% reduction in Annual Rate of Occurrence Audit-defensible verification at every remote operator access point and contractor credential issuance. Meets the identity foundation of TSA directive requirements.	CIO IT headcount stays flat as the mobile and contractor workforce scales Self-service absorbs the credential reset volume that historically pulled operators off the road and contractors off the yard.
--	--	--

Each outcome is produced by the same control, deployed once.

For Transportation, the cost of doing nothing is paid in physical consequence. In cargo that moves on a credential the operator never verified. In contractor access that travels further than the role was scoped for. In helpdesk calls that come from yards, tarmacs, and ports where the answer cannot wait. In federal directives that compliance teams cannot meet because the identity foundation is not in place. Each cost compounds with the next. Closing the gap once aligns operational continuity, contractor governance, and federal compliance under a single verified human layer.

The Compounding Effect

Every quarter the workforce identity gap stays open is another quarter of operational overhead absorbed, productivity hours lost, and actuarial exposure carried on the books. Each individual cost has been quantified in the prior section. Stacked over 24 months, the combined figure changes the conversation.

A 15,000-employee healthcare organization delaying 24 months absorbs roughly \$15.7M in combined costs across operational efficiency, workforce productivity, and Annual Loss Expectancy. Over the same 24 months, an organization that has deployed enterprise IDV recovers net savings exceeding \$14M after the cost of the platform itself. The annual license cost lands at roughly 2% of the manual TCO. Break-even is measured in weeks, not quarters.

15,000-employee organization. Cumulative cost across operational efficiency, workforce productivity, Annual Loss Expectancy, and hiring fraud (excludes OFAC categorical exposure).

INDUSTRY	MANUAL BASELINE (24 MO.)	COMPLIANCE-GRADE IDV (24 MO.)	ENTERPRISE IDV (24 MO.)	NET RECOVERED WITH ENTERPRISE IDV
Healthcare	\$15.7M	\$8.6M	\$1.3M	\$13.0M
Technology	\$13.9M	\$7.7M	\$1.1M	\$11.6M
Industrial Manufacturing	\$13.1M	\$7.2M	\$1.1M	\$10.9M
Education	\$10.5M	\$5.8M	\$0.8M	\$8.7M
Transportation	\$8.6M	\$4.7M	\$0.7M	\$7.2M
Hospitality, Retail & Consumer	\$8.2M	\$4.5M	\$0.7M	\$6.9M

Figures scale approximately linearly with workforce size. Annual license cost is included in the Enterprise IDV column and represents roughly 2% of manual TCO. Compliance-grade IDV retains 50–60% of baseline ALE and adds integration and maintenance costs not visible in headline savings. The gap between compliance-grade and enterprise-grade verification widens with every quarter of deployment.

Compliance-grade IDV does not close this gap. It clears the audit checkbox, but it retains significant residual ALE and carries hidden integration and maintenance costs that erode the headline savings. The gap between compliance-grade and enterprise-grade verification widens with every quarter of deployment, because the residual exposure compounds the same way the manual exposure does.

The decision calculus is straightforward. The cost of waiting is paid in full. The cost of acting is recovered in weeks. Every additional quarter the gap stays open adds a quarter of compounding cost the business does not get back.

From Cost to Control: How to Close the Gap

The math runs in a single direction. Inaction compounds. Action recovers.

The shift required to change that direction is smaller than it looks. The identity stack stays in place. The IdP keeps authenticating accounts. The ITSM platform keeps routing tickets. The HRIS keeps the system of record. The four cost dimensions in this report — operational efficiency, workforce productivity, Annual Loss Expectancy, and hiring fraud — are produced at four specific moments in the workforce lifecycle. What changes is a single addition: a verified human layer at the four moments where the existing stack assumes one — recovery, helpdesk, hiring, and elevated-privilege approvals.

That layer converts each cost dimension from a recurring expense into a recovered margin. Helpdesk volume drops. Workforce hours return. Annual Rate of Occurrence falls by an estimated 92%. Hiring fraud closes before access is provisioned, with verification records that hold under audit and under sanctions scrutiny.

The cost of inaction is paid quarterly. The cost of action is recovered in weeks. Every deferred quarter is another full quarter of the stack absorbed against a control the organization could have deployed in less time than a typical procurement cycle.

The status quo is an expensive option. It does not show up that way on a single budget line, which is why it stays in place.

CFO Total annual cost recovered: up to \$6.5M For a 15,000-employee enterprise. Annual ALE reduction: 92% of baseline. License cost lands at roughly 2% of manual TCO. Break-even measured in weeks, not quarters.	CISO 92% reduction in Annual Rate of Occurrence For identity-driven breaches. Audit-defensible verification at every recovery, helpdesk, hiring, and high-privilege approval moment. Verification records that hold under audit and under sanctions scrutiny.	CIO IT headcount stays flat as the workforce scales Self-service absorbs the helpdesk volume that has historically driven IT growth. A single platform replaces the patchwork of custom workflows that have accumulated as technical debt.	CEO Workforce identity becomes accountable rather than assumed AI agent actions trace back to a verified human authorization. The cost of inaction stops accumulating on the books.
---	--	---	--

Each outcome is produced by the same control, deployed once.

The cost is real. The exposure is current. The control exists. Every quarter the gap stays open is a quarter the organization paid for a problem it could have solved.

See what this costs at your organization.

Every figure in this report represents a typical organization within a sector. Your actual exposure depends on your workforce composition, identity infrastructure maturity, and regulatory environment.

A 30-minute calibrated TCO assessment produces a workforce-specific view of what the gap is currently costing you — and what closing it would return. No procurement commitment required.

Schedule your assessment

Methodology

Every figure in this report can be traced. Every calculation can be audited. Every assumption is named.

How This Report Calculates Cost

Every figure in this report is derived from Nametag's Total Cost of Ownership model, calibrated against published external benchmarks. The model is proprietary. The inputs that feed it are not.

The model translates organizational characteristics — workforce size, industry, identity event volume, and verification posture — into the four cost dimensions quantified across the report: operational efficiency, workforce productivity, Annual Loss Expectancy, and hiring fraud.

The figures are designed to give executives an order-of-magnitude view of what the workforce identity gap is costing their organization, calibrated against the most-cited industry sources in cybersecurity and workforce economics. They are a starting point for an internal modeling exercise, not a substitute for an actuarial analysis tied to a specific organization's incident history and regulatory environment.

Definitions Used Throughout the Report

Workforce identity gap	The structural gap between authenticating an account and verifying the human behind it. The four cost dimensions in this report are four expressions of that gap.
Operational efficiency	The IT labor and overhead burden of running manual identity verification.
Workforce productivity	The hours employees lose to identity friction across the workforce, valued at fully loaded employee compensation.
Annual Loss Expectancy (ALE)	The actuarial financial exposure tied to identity-driven breaches in a given year. Calculated as Annual Rate of Occurrence × Single Loss Expectancy.

Definitions Used Throughout the Report

Annual Rate of Occurrence (ARO)	The probability of a successful identity-based breach occurring in a given year, expressed as a percentage. Calibrated against industry breach frequency data.
Single Loss Expectancy (SLE)	The average financial cost of an identity-based breach when it occurs, calibrated against IBM's 2025 Cost of a Data Breach Report and sector-specific breach economics.
Hiring fraud	The identity risk and recruiting cost that enters the organization before an employee's first day, including OFAC sanctions liability for paying a sanctioned worker.
Enterprise IDV	Identity verification at the Stage 4 maturity posture — managed enterprise verification with continuous assurance across the workforce lifecycle, vendor-managed edge case resolution, and residual ALE in the single digits as a percentage of baseline.
Compliance-grade IDV	Identity verification at the Stage 2 maturity posture — point-in-time selfie matching, custom integration logic, and significant developer maintenance burden. Retains 50–60% of baseline ALE.

Inputs and Calibration

Identity event volume	Calibration: workforce size and industry-typical event frequency. Assumption: a 15,000-employee organization produces a sector-typical volume of password resets, MFA resets, account unlocks, hire events, and high-privilege approvals annually.
Per-event cost	Calibration: HDI 2025 helpdesk benchmarks for the manual baseline. Nametag deployment data for the enterprise IDV figure. Assumption: \$25 per ticket manual baseline, \$3.45 per ticket with enterprise IDV.
Workforce productivity loss	Calibration: US Bureau of Labor Statistics industry compensation data with a 1.4× fully loaded labor multiplier. Assumption: identity-friction hours multiplied by sector-specific fully loaded hourly rate.
Annual Loss Expectancy	Calibration: Single Loss Expectancy from IBM's 2025 Cost of a Data Breach Report. Annual Rate of Occurrence from the 2025 Verizon Data Breach Investigations Report and Sophos Active Adversary Report 2025. Assumption: identity-driven breaches occur at a sector-specific probability against a sector-specific average cost.
Enterprise IDV impact	Calibration: Nametag deployment data. Assumption: 92% reduction in Annual Rate of Occurrence. 86% reduction in per-ticket cost. 80% reduction in identity-friction hours. Applied as constants across all industries in this report.
Hiring fraud exposure	Calibration: 2025 Verizon DBIR, OFAC enforcement guidelines, and federal case data on state-sponsored employment fraud operations. Assumption: industry-typical fraud rate against sector-specific recruiting cost and a fixed-rate civil liability per OFAC violation.

Disclaimers and Limits

Every figure represents a typical organization within the named sector. Individual organizations carry exposure that varies based on workforce composition, regulatory environment, identity infrastructure maturity, geographic footprint, and threat surface.

The 24-month cumulative figures assume the workforce identity gap remains open across the period. Organizations that close the gap mid-period recover proportionally. Organizations that experience a successful breach during the period absorb the realized cost in addition to the cumulative inaction figures.

The Enterprise IDV impact constants (92%, 86%, 80%) reflect Nametag deployment data and are sector-typical rather than guaranteed for any individual deployment. Outcomes vary based on organizational adoption, integration depth, and the specific identity moments addressed.

OFAC civil penalty figures reflect the 2025 schedule and may change with subsequent updates.

This report reflects research conducted between January 2026 and May 2026. Organizations evaluating their own exposure can request a calibrated TCO assessment for their specific workforce profile.