turn

SOC 3® Report

Controls Related to Security
For the Period January 1, 2025 to December 31, 2025

Prepared in accordance with the attestation standards established by the American Institute of Certified Public Accountants

Table of Contents

Independent Service Auditor's Report

To the Management of Turn Technologies, Inc.
Chicago, Illinois

Scope

We have examined Turn Technologies, Inc.'s (the Company, or Turn) accompanying assertion titled "Assertion of Turn Technologies, Inc.'s Management" (assertion) that the controls within the Turn Platform (the Platform) were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the Platform to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled "Assertion of Turn Technologies, Inc. Management" about the effectiveness of controls within the Platform. When preparing its assertion, the Company is responsible for selecting and identifying in its assertion the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the Platform.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that the controls within the Platform were effective throughout the period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted following attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated in all material respects.

We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. We are required to be independent of the Company and to meet our other responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Platform were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

MJD Advisors

Waukee, Iowa
April 8, 2026

Assertion of Turn Technologies, Inc. Management

We, as management of Turn Technologies, Inc., are responsible for designing, implementing, operating, and maintaining effective controls within the Platform throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that the Company's service commitments and system requirements relevant to security were achieved. We have described the boundaries of the Platform in the section titled "Management's System Disclosures" (the System Disclosures), which identifies the aspects of the Platform covered by our assertion. The accompanying system disclosures, including the description of the platform's boundaries, principal service commitments, and system requirements, fairly present the platform covered by this assertion in all material respects.

We have performed an evaluation of the effectiveness of the controls within the Platform throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Our objectives for the Platform in applying the applicable trust services criteria are embodied in our service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the System Disclosures.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the Platform were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that our service commitments and system requirements were achieved based on the applicable trust services criteria.

Management of Turn Technologies, Inc.
April 8, 2026

Management's System Disclosures

Types of Services Provided

Turn Technologies, Inc. was founded in 2016 with a mission to create an AI-powered "workforce-as-a-service" platform (the Turn Platform or the Platform) designed to transform how organizations screen, verify, monitor, and manage contingent, hourly, and high-volume workforces. The Turn Platform is designed to support both regulated enterprise hiring needs and fast-moving contingent workforce programs by automating critical hiring workflows, improving speed-to-hire, and maintaining compliance with applicable laws and industry standards, including Fair Credit Reporting Act (FCRA) and Equal Employment Opportunity Commission (EEOC) guidance. The Company's focus is on supporting hiring organizations (partners) as well as the applicants consenting to background checks or utilizing other services (workers), which are the key users described in this system description. The Platform serves two primary customer categories: (1) direct employer partners, including high-volume and enterprise hiring organizations; and (2) HR technology platforms and ATS/HRIS vendors that embed Turn's screening infrastructure via TurnOS.

Services are delivered through a web-based partner dashboard, integrations with applicant tracking systems (ATS) and human capital management systems (HRIS), and API-based integrations, including TurnOS, Turn's embeddable screening infrastructure, which enables partners to automate, white-label, and embed screening and compliance workflows directly within their existing hiring systems.

Turn's technology supports the full pre-hire to post-hire lifecycle, including:

Service	Description
Pre-Employment Background Screening	Flexible, configurable checks that may include identity verification, SSN trace, nationwide and county criminal searches, sex offender registry checks, global watchlist checks, address history, and motor vehicle record (MVR) checks.
AI-Enhanced Screening Tools	Embedded AI features such as record matching, natural language interpretation of complex records, and AI Assistant guidance to improve accuracy, reduce false positives, and accelerate review and adjudication.
Drug Testing and Healthcare Sanctions	Integration and support for drug screening services and specialized healthcare and regulatory screenings as required by certain industries.

Service	Description
Continuous Monitoring & Post-Hire Compliance	Ongoing monitoring of critical data sources, including criminal and driving records (Continuous MVR), to notify employers of significant changes after initial hire.
Compliance and Audit Workflows	Automated adverse action procedures, compliance controls, and audit trails designed to help customers maintain adherence with FCRA and other legal requirements.
TurnOS (Infrastructure Layer)	An embeddable, AI-powered background screening infrastructure that enables HR platforms to offer white-labeled background checks directly within their product, retain program economics, and transfer compliance and operational overhead to Turn.

Boundaries of the Platform

The system boundary encompasses all components involved in the service lifecycle — including initiation, authorization, processing, recording, and reporting — for services provided to user entities through the Turn Platform. The system boundaries do not include instances in which transaction-processing information is combined with other information for secondary purposes internal to the service organization, such as accounting and billing.

The system boundaries do not include Turn's internal financial systems, employee HR and payroll systems, or the internal systems of subservice organizations. The policies, procedures, and controls of employer partners and HR platform partners are also outside the scope of this examination; however, certain controls are assumed to be implemented by user entities. See 'Complementary User Entity Controls' below.

Infrastructure

The Company's infrastructure is managed through a cloud hosting model with the primary services supported by Heroku and Amazon Web Services (AWS) (the Cloud Providers). The Company leverages the Cloud Providers to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Platform architecture within the cloud hosting environment to ensure security and resiliency requirements are met.

The specific services utilized to support the Platform's cloud infrastructure include the following:

Cloud Hosting Services

Service	Description
Heroku Postgres	Managed PostgreSQL database service
Heroku Config Vars	Environment variables management
Redis Cloud	In-memory data store (Heroku add-on)
New Relic APM	Application performance monitoring, root cause analysis
Elastic Cloud	Elasticsearch cluster hosted by Elastic Cloud (Heroku add-on)
Bucketeer	Heroku managed AWS S3 buckets
Google Cloud Firestore	Managed NoSQL document database service
Fixie	Static IP addresses for outbound requests
AWS S3	Object storage
Auth0	User authentication
Datadog	Monitoring and alerting
Datadog Security	Real-time threat detection and continuous configuration audits

Certain controls of Heroku and AWS are necessary in combination with the Company's controls to provide reasonable assurance that the Company's service commitments and system requirements are achieved based on the trust services criteria (Complementary Controls). The Company is responsible for the oversight and monitoring of Heroku and AWS, which is performed through the vendor management policies and procedures.

The following are the applicable trust services criteria and controls that are necessary to be in place at Heroku and AWS to provide reasonable assurance that the Company's service commitments and system requirements were achieved:

Complementary Controls

Criteria	Control
Logical and Physical Access CC6 Series	Procedures are implemented to authenticate authorized users, restrict physical and logical access, and detect unauthorized access attempts and procedures are implemented to decommission and physically destroy production assets securely. Security measures are implemented to provision and deprovision user access to systems and applications based on appropriate authorization, and encryption has been implemented, by default or as configured by the Company, to secure the transmission and storage of information.
System Operations CC7 Series	Vulnerability scans and penetration testing are performed periodically to identify system vulnerabilities, and environmental protection, monitoring, and procedures for regular maintenance are implemented at the data center facilities. Incident response procedures are established and implemented to identify, analyze, and remediate events and incidents.
Change Management CC8 Series	Procedures are established and implemented to ensure system changes are authorized, designed, developed, configured, documented, tested, and approved before production deployment.

The examination performed by the independent service auditor did not extend to the policies, procedures, and controls of Heroku and AWS.

Complementary User Entity Responsibilities

The Platform has been designed utilizing a shared responsibility model where certain controls should be implemented by user entities (employer partners and HR platform partners) to meet best practices. These controls include the following: (1) User entities are responsible for managing and securing their own API credentials and access tokens. (2) User entities are responsible for provisioning and deprovisioning authorized users on a need-to-know basis. (3) User entities are responsible for the accuracy of configuration data (e.g., screening package selections) submitted to Turn. (4) User entities operating ATS/HRIS integrations are responsible for implementing TLS/HTTPS for all API calls. (5) User entities are responsible for maintaining their own incident response procedures for security events affecting data processed by the Turn Platform.

Software

Software consists of the applications and supporting tools used to build, operate, secure, maintain, and monitor the Platform. The principal software includes the following:

Software Summary

Application	Purpose
Drata	Compliance management platform
Jira	Project management and issue tracking
Bugsnag	Error monitoring and application stability monitoring
Google Workspace	File storage, email, document collaboration, identity provider
GitHub	Source code repository
GitHub Actions, Semaphore	CI/CD
GitHub Dependabot	Dependency scanning
Twilio	Communication API
Stripe	Billing
Mandrill	Transactional email
Mode	Business intelligence
Gusto, Freshteam	Human resources information system and management

Application	Purpose
Freshdesk	Customer support
Freshping	API endpoint performance monitoring
BriteVerify	Email verification and validation
OpenAI	Managed large language model (LLM) services
Papertrail	Log management
Google Analytics	Website analytics
Slack	Communication hub

AI Systems

The Company utilizes managed LLM services provided by OpenAI (the AI System) to enhance its background screening and criminal record analysis platform by performing disposition classification and legal insight extraction from criminal records. These capabilities support the review and adjudication workflows by categorizing complex legal outcomes, specifically those involving plea agreements, into standard classifications like "conviction" or "non-conviction." AI-generated classification outputs are used as decision-support tools and are subject to human review prior to any adverse action determination.

Services are accessed through direct API integration with endpoints where only raw, anonymized disposition text is processed. The integration is configured to ensure no personally identifiable information, applicant names, or internal tracking IDs are shared with the provider, and AI classification results are cached locally within the Turn Platform to minimize repeated transmission of data to external systems and to maintain operational continuity.

People

The Company's organizational structure provides the framework for the management, operation, and security of the Platform. Where an individual serves in multiple roles, the Security Committee provides independent cross-functional oversight to maintain appropriate separation of responsibilities. All personnel with access to production systems or sensitive candidate data are required to complete background screening and annual security awareness training prior to and during their tenure.

Organizational Structure

Role	Function
Board of Directors	Responsible for governance, oversight of management, and major decision making, representing the interests of shareholders and includes members independent of management
CEO	Responsible for oversight of the development and performance of internal controls and the direction of company-wide activities
CISO	Responsible for the design, development, maintenance, dissemination, and enforcement of the Information Security Program
Security Committee	Cross-functional team responsible for oversight, implementation, and continual improvement of the Information Security Program
Business Operations	Manages internal business needs such as human resources, customer success, and other administrative functions
Legal	Responsible for compliance and legal functions of the Company, including external attorneys providing services under management supervision
Engineering Team	Responsible for the development, testing, deployment, and maintenance of the Platform and for maintaining security

Procedures

Procedures are the specific actions undertaken to implement defined processes and achieve system objectives. Information security policies are owned by the CISO, reviewed at a minimum annually, and communicated to all applicable personnel through onboarding and recurring security training. The Company has adopted the following information security policies relevant to the Platform:

> Acceptable Use Policy
> Asset Management Policy
> Backup Policy
> Background Check Compliance Policy
> Business Continuity Plan
> Change Management Policy
> Code of Conduct
> Data Classification Policy
> Data Protection Policy
> Data Retention Policy
> Disaster Recovery Plan
> Encryption Policy
> Incident Response Plan
> Information Security Policy
> Logging and Monitoring Policy
> Password Policy
> Physical Security Policy
> Responsible Disclosure Policy
> Risk Assessment Policy
> Software Development Lifecycle Policy
> System Access Control Policy
> Vendor Management Policy
> Vulnerability Management Policy

Data

Data refers to the transaction streams, files, data stores, tables, and output used or processed by the Company. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established with customers and business partners. The following table details the types of data collected by the Company in connection with the Platform's services and the infrastructure, software, and third-party vendors utilized to store and process the data.

Data Type Summary

Type	Description	Storage and Processing
Applicant / Worker Data	Personally identifiable information necessary to apply for open positions, sourcing, and perform background checks as well as the results of background screening services performed	Heroku, AWS, Freshdesk
Partner data	Personally Identifiable Information and other administrative data from personnel, customers, and other third parties	Heroku and other third-party technology providers
Secrets	Access credentials, tokens, certificates, API keys, and other secrets	Auth0, Heroku Config Vars
Log information	Information relevant to and explicitly necessary for services, including metadata	Datadog, New Relic APM, Papertrail
Analytics data	Product usage and tracking data are sent to analytics services to analyze usage patterns and inform product decisions	Google Analytics

Customer data is retained in accordance with Turn's Data Retention Policy and applicable regulatory requirements, including the FCRA. Consumer report data is retained for the minimum period required by applicable law and deleted upon expiration or verified deletion request. Log and audit data are retained for a minimum of 12 months to support incident investigation and compliance monitoring.

Principal Service Commitments and System Requirements

The information presented within the Boundaries of the Platform was prepared to describe the procedures and controls the Company implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The disclosure of the principal service commitments and system requirements enables report users to understand the critical objectives that drive the system's operation.

Service Commitments

Service commitments include those made to user entities and others (such as customers of user entities) to the extent those commitments relate to the trust services category or categories addressed by the description. Security objectives and commitments are made available to workers and partners through managed services agreements and information shared on the Company's website. The following summarizes the Company's principal service commitments that management believes to be relevant to the report users:

- The Company implements a documented Information Security Program, regularly tested through an independent SOC 2 Type II examination, to protect customer and candidate data against unauthorized access, disclosure, and misuse.
- Customer personally identifiable information (PII) is encrypted with AES 256-bit encryption.
- Access to critical resources and sensitive information requires multi-factor authentication and is provided based on the principle of least privilege.
- The Company continuously monitors access to its infrastructure using SIEM tooling, real-time threat detection (Datadog Security), and application performance monitoring (New Relic APM, Datadog), with alerts configured to notify the Security Committee of anomalous activity.
- Data transmitted between the Platform and external systems is encrypted using HTTPS/TLS.

System Requirements

The Company's system requirements are communicated in system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data and include descriptions and expectations for the system's design, development, and operation. In addition to these policies, standard operating procedures have been prepared to describe specific manual and automated processes required to operate and develop the services provided.

System requirements include: (1) all production code changes must pass automated testing and peer review before deployment; (2) all production infrastructure changes must be authorized through the change management process; (3) access to production systems is provisioned based on job role and deprovisioned within 24 hours of role change or termination.

Turn Platform Architecture

Turn's platform is built on a cloud-native architecture, hosted across Heroku and AWS, designed with a defense-in-depth approach that separates data storage, application logic, and access management across independently secured layers.

To provide transparency into this architecture, Turn maintains a set of C4 diagrams that clearly document system boundaries, components, and interactions across the platform. The C4 Level 1 Architecture Diagram included in this section offers a high-level view of the system landscape, illustrating how core infrastructure, services, and external dependencies work together to support secure operations. Turn updates these diagrams as the Platform evolves.

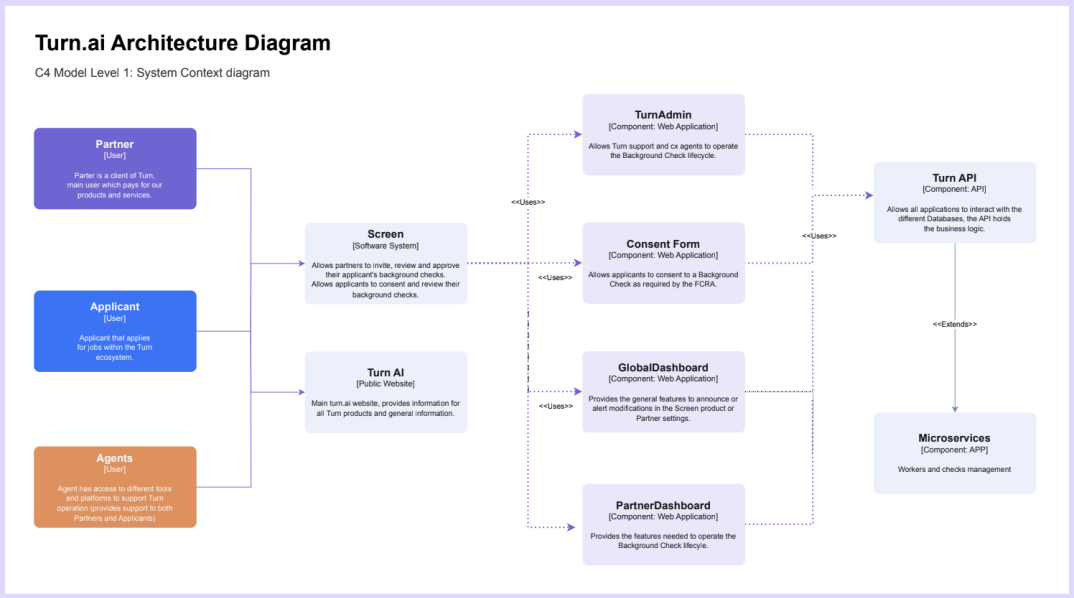

Figure 1: The C4 Level 1 diagram illustrates the primary system components depicting its relationships with the users and external systems that interact with it.

In addition to the Level 1 diagram presented here, Turn maintains more detailed C4 diagrams (Levels 2–4) that provide deeper insight into containers, components, and code-level architecture. These diagrams are available upon request to customers, auditors, and partners who require a more granular understanding of the Platform's design, further demonstrating Turn's commitment to transparency, security, and continuous improvement.

Turn Platform Screenshots and User Experience

The following screenshots illustrate the Turn partner dashboard, demonstrating the controls and workflows described in this report as they appear to authorized users. The dashboard provides HR administrators and platform partners with real-time visibility into screening status, role-based access management, and audit-ready reporting, enabling compliance oversight to be exercised directly within the hiring workflow.

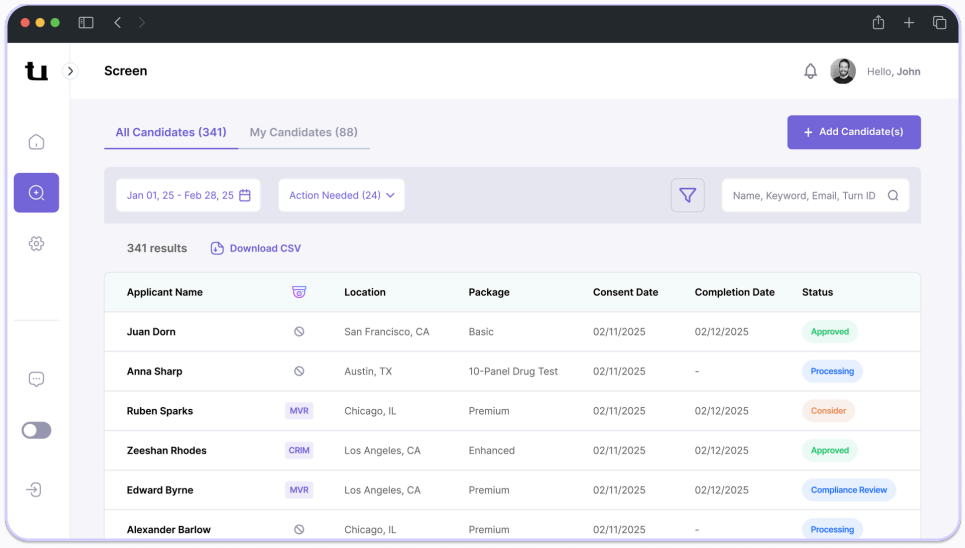

Figure 2: Turn Partner Dashboard screening pipeline advanced search controls.

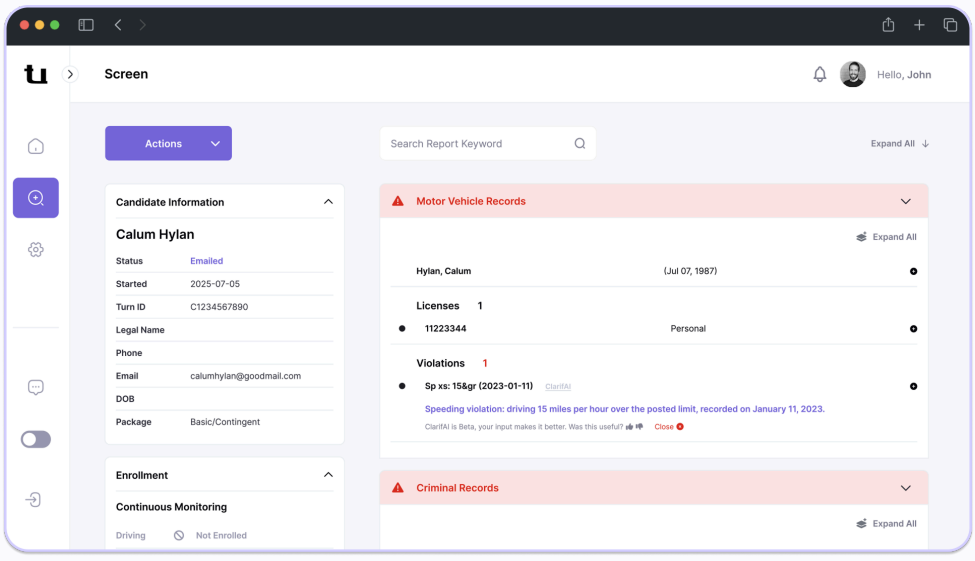

Figure 3: Applicant Report - actionable actions, and check-level hit display with AI assistance.

Note: These screenshots are included for general informational purposes and should not be interpreted as a comprehensive description of all platform features or controls.

Building Trust Through Security: Customer Perspectives

The following perspectives are from Turn customers who have evaluated the platform's security posture as part of their vendor onboarding and ongoing partnership. They represent the direct-employer and workforce-platform segments of Turn's customer base.

> "Hiring is built on real relationships. Candidates decide whether they can trust you long before there's an offer on the table, and part of earning that trust is how we protect their personal information. We hold ourselves to a high standard, and we expect the same from our partners. Turn's SOC 3 report reassured us that they approach privacy and security with the same care and integrity we bring to every candidate interaction. That matters to our candidates, and it matters to us."

Katie Gottlieb

VP, Talent Acquisition at SiteOne Landscape Supply

Turn's public SOC 3 report is the summary of the underlying SOC 2 Type II examination — a full-year independent audit of operating control effectiveness. Partners who require the complete Type II report with detailed control testing results may request it directly.

> "Every vendor we onboard is a potential entry point. Background check providers are especially high risk because the data they handle is exactly what bad actors want. We have worked with Turn for nearly a decade, and their SOC 2 Type 2 report is part of what gives us continued confidence year after year. A full year of independent testing, not a self-assessment. We don't take vendor security on faith."

Zachary Hensley

VP, Product & Operations at FRAYT

Why Security Matters: The Business Case for Verified Controls

For high-volume employers and HR platforms, a security incident is not simply an IT issue. It can disrupt hiring operations, expose highly sensitive candidate and employee data, create legal and contractual obligations, and undermine trust across the hiring ecosystem.

The Financial Impact of a Data Breach

The financial stakes are significant. IBM's Cost of a Data Breach Report 2024 found that the global average cost of a breach reached **$4.88 million**, a record high driven by business disruption and post-breach response costs. In the United States, breach costs are considerably higher. IBM's 2025 report placed the average U.S. breach cost at **$10.22 million**, reflecting increased regulatory penalties and extended detection timelines. Seventy percent of breached organizations reported that the breach caused significant or very significant operational disruption, and the average time to identify and contain a breach was 241 days.

Recent Security Failures in the Screening Industry

Background screening and employment verification workflows involve some of the most sensitive data an organization handles: Social Security numbers, government-issued IDs, financial account information, criminal records, and employment histories. When security controls fail in this space, the consequences are immediate and severe.

Recent events in the screening ecosystem illustrate this clearly:

- **A major employment screening provider** serving over 55,000 companies, including 30% of Fortune 500 companies, disclosed a breach affecting **3.3 million individuals** in early 2025. An unauthorized actor remained undetected on its network for over two months. The exposed information included names, Social Security numbers, driver's license numbers, and financial account data. The company now faces multiple federal class action lawsuits alleging failure to implement reasonable security practices and unreasonable delay in notification.

- **A background check data broker** that offered screening services via API suffered a breach involving an alleged dataset of approximately 2.9 billion records, including Social Security numbers, addresses, and dates of birth. The stolen data was listed for sale on the dark web for $3.5 million. The resulting legal exposure, including class action lawsuits, state attorney general investigations, and a congressional inquiry, proved catastrophic. By October 2024, the company had filed for Chapter 11 bankruptcy, explicitly citing the cyberattack as the cause, with its insurer declining to provide coverage.

These outcomes are not isolated events. The FTC has pursued enforcement actions against screening companies for Fair Credit Reporting Act violations, including a $2.6 million civil penalty against one of the industry's largest providers required under the Fair Credit Reporting Act, including requirements related to accuracy, consumer disclosures, and reinvestigation of disputed information.

Vendor Risk Is Customer Risk

For employers and HR platforms, a vendor's breach does not stay the vendor's problem. As Littler Mendelson notes, when a business vendor suffers a data breach involving employer data, breach notification laws impose ultimate responsibility for breach response on the employer-customer, not just the vendor. The vendor's statutory responsibility is generally limited to informing the employer of the breach. This puts the employer in a difficult position: it holds the legal obligation to notify affected individuals, but may lack the information needed to do so properly.

In practice, this means the security posture of a screening provider directly affects the employer's legal obligations, brand reputation, and ability to maintain business continuity. Security diligence on screening vendors is not a back-office preference. It is a procurement requirement.

Independent Verification as a Foundation of Trust

This is why independent validation matters. A SOC 2 Type II audit examines whether security, availability, and confidentiality controls are not only designed but operating effectively over time. A public SOC 3 report extends that transparency to customers, prospects, and partners who need assurance without requesting a full audit report under NDA.

Turn Technologies has completed a SOC 2 Type II attestation, and this SOC 3 report represents the public summary of those controls and findings. For teams managing high-volume hiring workflows, where sensitive candidate data moves through screening systems every day, verified security controls are foundational to protecting data, preserving customer confidence, and keeping hiring operations running without interruption.

Thank you

Contact

support@turn.ai

Our address

311 W. Monroe St. 3rd Floor
Chicago, IL 60606

Made with ❤ in Chicago