EQUIFAX®

# 2023 Security Annual Report

We've embedded **security into everything we do**, from our employee engagement and M&A strategy to our technology infrastructure, custom data fabric, new product development, and EFX.AI approach.

Mark W. Begor

Chief Executive Officer
Equifax

# Trusted Data Stewardship Is More Important Than Ever

As we move closer to completing the Equifax Cloud,™ we are leveraging our new Cloud capabilities, single data fabric, differentiated data, and EFX.AI Artificial Intelligence to deliver new solutions for customers and consumers in each of the 24 markets we serve. Our company purpose of helping people live their financial best and our commitment to being consumer friendly at every touchpoint guide our business actions.

Over a decade of EFX.AI innovation is fueling our momentum. Equifax has 90+ patents supporting our approach to AI and machine learning (ML), and we infuse our patented AI techniques into product development and delivery to enable customers to get to insights faster. The successful use of AI requires deep, accurate, and high-quality data — making trusted data stewardship, enabled by strong cybersecurity, more important than ever.

Over the last six years, we have built one of the world's most advanced and effective cybersecurity programs. The maturity of our cybersecurity program increased again in 2023, outperforming all major industry benchmarks for a fourth consecutive year. And, our security posture score continues to exceed Technology and Financial Services industry averages.

We've achieved this leadership by embedding security into everything we do, from our employee engagement and M&A strategy to our technology infrastructure, custom data fabric, new product development, and AI approach. Regardless of role, security is each of our jobs, and we all put security first.

As we continue our security leadership journey, we continue to share our learnings and collaborate closely with customers, policymakers, and other organizations — helping shape the future of cybersecurity to better protect our own data while simultaneously moving the whole industry forward. As our 2023 Security Annual Report outlines, change is constant — and when it comes to preparing for what's next in cybersecurity, it's imperative that we, and our partners across the world, continue to raise the bar. We remain committed to being an **industry leader in cybersecurity.**

# Fast, Adaptable, and Relentless

The ingenuity, speed, and spectrum of cyber attacks staged in the last year — ranging from rudimentary to sophisticated — underscore the scope and scale of the fight we're in as cyber defenders.

Whether it was high-tech AI deepfakes in video meetings or low-tech help desk social engineering, the cyber landscape highlighted attackers' all-too-successful playbook: Use cutting-edge tech when you can, and be basic when it suits you. But above all else, be relentless and adapt quickly.

**We adopted a similar mindset in 2023.**

When we discovered hackers targeting IT help desks at other companies, we quickly developed a groundbreaking new use case for our passwordless platform — biometric caller authentication — eliminating 94% of knowledge-based authentication (KBA) in just two months.

When we anticipated the impending threat of AI deep fakes leading to corporate fraud, we proactively trained our people on the potential risk and began work on a technical solution, months before any corporate victims even emerged.

When vendors didn't have patches for newly announced vulnerabilities, our global teams quickly implemented creative mitigating controls to address the risk, often within 24 hours.

All of these were quick adaptations, leveraging cutting-edge tech where possible and relying on resourcefulness when needed.

Our security posture in 2023 was undoubtedly tied to Equifax tech and talent investments, but it's our commitment to constant improvement and quick adaptation that truly sets us apart — for big initiatives and short-fuse fixes alike.

I'm really proud of the progress our Equifax team made in 2023. **We're better positioned than ever to protect our people — employees, customers, and consumers.**

Jamil Farshchi

Chief Information Security Officer
Equifax

# **Our Impact:**
# Equifax Security in 2023

**12 million+**
Cyber threats defended against on average each day

**222,000+**
Simulations launched to test our global workforce in security

**23,000+**
Employees and contractors received personalized security training

**7,500+**
External users accessed our security and privacy controls framework

**2,800+**
Customer questionnaires and audits completed

**1,900+**
Deep-dive risk analyses on critical and high risk third party vendors

**600+**
Organizations supported via Equifax Breach Services, with identity protection offered to more than 13.5M breach victims in 135 countries on behalf of our clients

**400+**
Cybersecurity professionals protecting consumer data

**320+**
Automated cloud security checks monitored in real time

**100+**
New Product Innovations (NPIs) securely brought to market for the fourth consecutive year

**50+**
Forums participated in to tackle global cyber challenges

**51**
Certifications and authorizations obtained from outside auditors

**45**
Physical security assessments completed, validating appropriate controls

**16**
Tabletop exercises held to prepare for crisis scenarios

**8**
Acquisitions fully integrated from a security standpoint

**4**
Consecutive years achieving a Security Maturity score that outperforms all major industry benchmarks

# State of Play:
# Cybersecurity in 2023

The themes below are representative of the prevalent themes of the past year.

### Past is Prologue

Many of the threats we detailed in our previous annual reports — ransomware, Multi-Factor Authentication (MFA) bypass attacks, supply chain vulnerabilities, and large-scale attacks on nations — remain both pervasive and increasingly sophisticated, causing the number of data breaches in 2023 to surpass the previous high by more than 70%.[1] This increase is a reminder that, as new risks emerge, existing risks must be prioritized with equal vigilance.

### Credentials Crisis

In 2023, a targeted attack against an identity and access management (IAM) vendor demonstrated the challenges of defending against the growing threat of identity-related attacks. Whether through phishing, social engineering, or credential stuffing, nearly every industry was impacted, with attacks sweeping the entertainment, consumer goods, and biotechnology sectors and beyond.

### AI Exploration

Security teams saw instances of AI-enabled voice and even video cloning, where hackers realistically impersonated business leaders and instructed employees to take unauthorized actions, costing businesses millions. Prudent teams also quickly established that all AI is not created equal — internal AI formulas with propriety, curated data are much lower-risk and higher-impact than external AI solutions relying on public datasets and generic algorithms.

### Governance Imperative

Across the world, government bodies worked to increase security accountability. Among them was the U.S. Securities and Exchange Commission (SEC) rules on the annual disclosure of material information regarding cybersecurity risk management, strategy, and governance. Following the announcement of these rules, a ransomware gang filed an SEC complaint against a company they breached, alleging that the company failed to report the attack in a timely manner.

As new risks emerge, existing risks **must be prioritized** with equal vigilance.

[1] Identity Theft Resource Center, 2023 Data Breach Report

# **Our Actions:**
# Equifax Security Initiatives and Results in 2023

### Reinforced Our Internal Security Culture

Security is in our DNA. At Equifax, we believe that Security is everyone's job, and we continued to put strong security education into practice by **launching 222,000+ simulations** to safely gauge how our workforce responds to various security scenarios such as phishing attacks.

We engaged our workforce through a record-breaking internal **Cybersecurity Awareness Month** campaign, with thousands of employees testing their cyber knowledge and familiarizing themselves with key security-related materials.

We also **enhanced our employee security scorecard** to enable more tailored measurement of key behaviors (such as data handling and secure browsing) and introduced impact-based weighting to reinforce proper risk-based prioritization.

### Strengthened Continuous Control Governance

We further **standardized the way we measure our control posture and performance**, ensuring a structured and reliable assessment of our security measures.

**Quantifiable and continuous security risk scoring** helped drive stronger alignment on priorities and more efficient execution of security improvements.

And we upgraded to a next-generation cloud security platform that **weaves controls into processes** within The Equifax Cloud,™ making it easy for users to do the right thing.

### Increased Efficiency

By automating rote components of workflows (while maintaining human oversight) and driving **process improvement**, response times (and times to complete routine tasks) are universally down.

We reduced **threat hunt analysis** time (by 87.5%), **security operations center** response time (by 99.6%), and **data loss prevention support ticket** processing time (by 75%). We automated **device detection** and more.

## Accelerated Frictionless Security

Kicking off our **journey to passwordless logins** — and our move to replace employee credentials with biometrics across a variety of applications and systems, we enacted interactive voice response (IVR) authentication when employees call into our HelpDesk, eliminating the weakest, most easily social engineered credentials within companies today.

To enhance operational efficiency, we introduced a **1-click email approval option** within our internal access entitlements platform, reducing administrative time while maintaining robust authentication protocols.

And through a cross-functional, integrated effort called the Compliance Automation Program (CAP), we've **ingrained our application security requirements** deeply into the Equifax Cloud.™

## Fueled Business Growth

We obtained **34% more certifications** than in 2022 while reducing cost per certification by 19%, harmonizing controls and reusing evidence. This allowed us to better meet current and prospective customers' requirements.

As part of these efforts, we developed an **assessment process for state compliance frameworks**, enabling Equifax to better serve state governments across the U.S. in the Cloud.

And we made it even easier for our customers to validate the security of their **Equifax Cloud-based products and services**, enabling them to map the policies they see in their CloudControl dashboard to the policies' corresponding controls in the Equifax Security Controls Framework.

## Expanded External Collaboration

We **drove productive security dialogue with a range of stakeholders** — with students at University of California, board members at the New Zealand Institute of Directors conference, officials at the Costa Rican Ministry of Technology, finance leaders on the CNBC CFO Council — and at dozens of other locations and topics in between.

This dialogue was followed by action. For example, we helped launch a **nationwide cybersecurity awareness course** in Costa Rica. We also became one of the few — if any — public companies to **open-source our security and privacy controls framework**, which has since been accessed by 7K+ users in 95+ countries.

# Accelerating Security at Scale

We accelerated the scale of our security program — enabling our practices to be incorporated by many other stakeholders — through co-design, public-private partnerships, and transparency.

## Cascading our approach:

### through co-design with vendors

**We helped advance a better way to conduct supply chain security.**

Launched in 2022, Equifax CloudControl gives our customers real-time visibility into the security of the cloud products they use from us. While that's an industry first, we don't want to be an outlier.

To spur broader industry change, we worked side by side with our vendor to build a new version, maturing it toward a stage where other companies can use the same solution to offer their customers this real-time visibility, working to help move the industry away from reliance on questionnaires.

**We developed a first-of-its-kind approach to help desk authentication.**

When employees call Equifax technical support, they can now use a mobile app to automatically authenticate and connect with an agent. That capability didn't exist out of the box — weaker forms of multifactor authentication are the norm for help desks today.

We worked to find a vendor who shared our vision for a better way. And we partnered to build this capability into their offering, paving the way for their other customer organizations to leverage the tool.

### through public-private partnership

**We partnered with the government of Costa Rica to train its citizens.**

The in-house Equifax Cybersecurity Awareness & Training team is dedicated to helping our employees and contractors follow security best practices. This team worked with the Costa Rican National Training Institute and Ministry of Technology to launch a free, nationwide virtual training course on best practices for everyday digital security.

We believe that individual companies should help drive broader education, because when the general public takes actions to reduce online risk, everyone benefits.

**We continued working closely with the FBI and CISA.**

In 2023, the Cybersecurity and Infrastructure Security Agency (CISA) and The Federal Bureau of Investigation (FBI) gave us intelligence into how a well-known ransomware group was planning to attack Equifax. We tailored our countermeasures. The threat arrived as we were warned, and the team was prepared.

CISA and the FBI provide this intelligence for a range of companies. The key is to proactively build relationships. Opening lines of communication, listening to input when it is received, and knowing what to do when you hear something are critical.

with a dedication to transparency

### We published our Security and Privacy Controls Framework.

With the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and Privacy Framework (NIST PF) as our foundation, we built an integrated, interactive, industry-leading framework, adding actionability and accountability via technical requirements. We published this framework to help others build or enhance their own cybersecurity programs.

It's been accessed by 7.5K users at companies ranging from Fortune 500 companies to startups and small nonprofits in 95 countries. Many users cross-referenced our framework against their existing ones, pinpointing areas where they can augment their programs with some of the controls we use in ours. Prior to our public release of this material, some smaller organizations didn't even have a framework due to the time and effort it requires.

### We helped the security compliance community minimize efforts and costs.

The Payment Card Industry Security Standards Council (PCI SSC) has stringent requirements for keeping customer card data secure. We are committed to fully complying with these standards in the most efficient, cost-effective way possible.

This commitment drove our development of comprehensive guidance detailing 15 advanced patterns that simplify compliance for systems regulated by PCI standards. Consequently, we were invited to join the PCI Council's Special Interest Group for segmentation, where Equifax guidance is being incorporated into PCI's upcoming standards revision. Sharing our internal approach is leading to industry change.

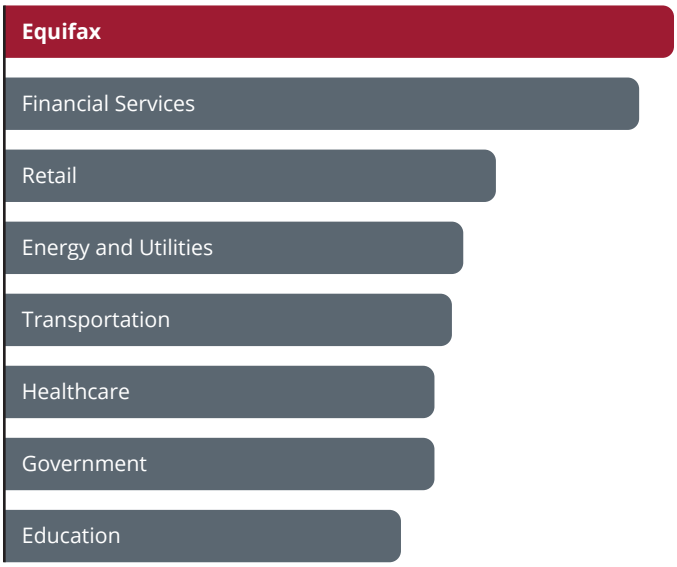
Cascading our approach through co-design with vendors, public-private partnership, and a dedication to **transparency**.

# Independent Benchmarking

## Security Maturity

A leading global research and advisory firm conducts annual in-depth analysis of the maturity of our entire security program.

**Security Maturity Score**




**What is Security Maturity?**

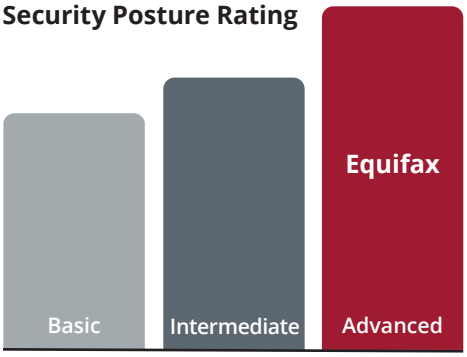
An organization's security maturity represents how well it can adapt to cyber threats and manage risk over time.

The maturity of our cybersecurity program improved in 2023, outperforming all major industry benchmarks for a fourth consecutive year.

## Security Posture

A leading cybersecurity reporting service continuously monitors the posture of our security program and assesses the risk of our supply chain ecosystem.

**Security Posture Rating**




These are the rating categories assigned by the reporting service that monitors our posture. Equifax maintains a rating that places us in the highest category.

**What is Security Posture?**

An organization's security posture is its readiness and ability to identify, respond to, and recover from security threats and risks.

Our security posture score capabilities exceeded Technology and Financial Services industry averages for a third consecutive year.

# **Summary of Results:** Equifax Security in 2023

## Security Posture and Maturity

Achieved a record Security Maturity score as measured by a leading global research and advisory firm, outperforming all major industry benchmarks for a fourth consecutive year

Achieved a Security Posture rating that exceeded Technology and Financial Services industry averages for a third consecutive year

## Cybersecurity

Monitored 321 automated cloud security checks in real time, driving greater visibility into the posture of our cloud estate

Consolidated Security Operations Center and Cyber Incident Response Team functions, creating a tiered model for 24x7 detection and response across the whole lifecycle; reduced time to respond by 99.6%

Enforced MFA for 100% of remote access to our network, reducing the risk of unauthorized entry

## Compliance

Obtained 51 certifications (a 34% increase over 2022) from outside auditors, validating our compliance with business, legal, contractual, and regulatory requirements

Achieved savings of 3,150 hours through compliance automation and control harmonization while still maintaining robust human oversight

Aligned execution of audits to achieve efficiencies, resulting in a 29% evidence reuse rate

## M&A

Aligned 8 acquisitions to corresponding Equifax business units and/or international regions with accelerated integration timelines and stronger cost controls without loss of core security requirements

Conducted robust due diligence on 3 efforts (including Boa Vista Serviços); efforts included comprehensive vulnerability scanning, code review, compromise assessment, and key control reviews prior to close

## Risk Management

Conducted deep-dive risk analyses on 100% of our company's critical and high risk third parties (1,970)
Completed risk assessments on 100% of business applications (6,453)

Established a quantitative real-time risk scoring foundation that is reviewed by management at regular intervals, helping to align security and technology priorities

## Crisis Management

Conducted 16 tabletop exercises and real-time crisis simulations with company stakeholders. Key stakeholders included:
– CEO and Executive Team
– Regional and Business Unit Crisis Teams

Introduced new employee resources to support our ongoing commitment to the safety and security of our employees. Key enhancements included:
– Revised emergency response plans
– Quick reference guides for emergency response
– Enhanced training materials

## Security Training

Conducted 210,406 global and 12,169 targeted simulations to test our workforce's response to potential security concerns

Maintained a market-leading aggregate security awareness score of 91.9, outperforming industry benchmarks

Drove increased workforce resiliency against phishing; enterprise achieved a 59.5% report rate (up 16.2% from 2022)

Enhanced our employee security scorecard to enable more tailored measurement of key behaviors (such as data handling and secure browsing) and introduce impact-based weighting to reinforce proper risk-based prioritization

Deployed a simplified, user-friendly intranet hub, "Security Central," where users can reach the 24/7 security hotline, find their functions' dedicated information security officers, and access policies, controls, FAQs, and more

Established a quantitative real-time risk scoring foundation, helping to align security and technology priorities

# Summary of Results

## Breach Services

Supported 608 organizations and their customers and employees, helping them respond to and recover from cyber incidents

On behalf of our clients, offered identity protection to more than 13.5M breach victims in 135 countries

## Customer Engagement

Completed more than 2,800 customer questionnaires and audits to ensure compliance, increasing questionnaire throughput by 51%

Launched version 2 of CloudControl, a first-of-its-kind solution that gives customers real-time visibility into the cybersecurity posture of their Equifax Cloud™-based products and services
- A new feature allows users to map the policies they see in CloudControl to their corresponding controls in the Equifax Security Controls Framework

## Products and Services

Securely brought 100+ New Product Innovations (NPIs) to market for the fourth consecutive year

Developed a streamlined Texas Risk and Authorization Management Program (TX-Ramp) assessment process, replicable across state compliance frameworks, enabling Equifax to better serve state governments across the U.S. in the Cloud

## Privacy

Reduced Cloud onboarding time by automating Data Classification while helping ensure consistent application of Data Protection Controls

Consolidated device control tools into a single platform, driving consistency across the enterprise for managing access to external devices

Published a global Employee Privacy Statement outlining how we collect, process, and store employee personal data

## Fraud

Streamlined processes and consolidated tools to drive increased fraud detection and mitigation, protecting over 150K consumers (405% increase versus 2022)

## Physical Security and Investigations

Completed 45 physical security assessments and 16 physical penetration tests, validating that appropriate controls are in place to protect employees, data, and assets

Through enhanced processes and automation, our Physical Security Operations Center bolstered our response time for local high priority alarms: within 3 minutes (13% faster response than 2022)

## Talent and Diversity

Continued to promote inclusivity within our workforce; 59% of our U.S. security team members represent diverse backgrounds, and 31% identify as female (vs. 24% industry average)

12 employees graduated from the Women Amplifying Voices in Equifax Security (WAVES) 2023 1:1 mentoring cohort

The Human Rights Campaign (HRC) recognized Equifax as a Best LGBTQ+ Employer in their 2023 Corporate Equality Index report; two Security team members helped earn this recognition through their roles on the board of the Equifax PRIDE employee resource group

## Advocacy and Partnership

Participated in more than 50 forums to promote stronger cybersecurity practices for business, government, and society

Developed comprehensive guidance detailing 15 advanced patterns that help remove/reduce compliance costs/efforts for systems regulated by the Payment Card Industry (PCI) standards; partnered with the PCI Council to cascade these efforts across the broader compliance community

Open-sourced our security and privacy controls framework, which has since been accessed by 7K+ users in 95+ countries

Partnered with the Costa Rican National Training Institute and Ministry of Technology to launch a free nationwide virtual cybersecurity awareness course

Released inaugural Australia and New Zealand Security Pulse Report detailing state of security in the region

Addressed legislative assistants for the House Committee on Energy and Commerce to provide input and show support for the American Data Privacy and Protection Act (ADPPA)

On behalf of our clients, offered identity protection to more than 13.5M breach victims in 135 countries

# **Finish line? Not in security.**
# Our Priorities in 2024

### Eliminating Secrets

We're shifting away from the traditional paradigm of authentication that relies on static, secret passwords toward more dynamic, inherently secure methods. We'll replace employee credentials with biometrics across a variety of applications and systems for unparalleled security, usability and time-saving benefits.

### Minimizing Supply Chain Risk

Third party attacks continue to surge, increasing the need to validate the security and compliance level of our vendors. New tools and processes are enabling us to gain a more comprehensive view of vendors and their risk postures. We'll also optimize our methods for holding vendors accountable to our industry-leading standards.

### Doubling Down on AI

In 2024, we'll continue to harness the positive benefits of AI. We see it as more than just a means to optimize and automate processes. It's a tool to enhance our understanding and preparedness. We'll use AI to synthesize data and test our security posture, providing a truly comprehensive view that accounts for changes, challenges and scenarios traditional rule-based systems might overlook.

equifax.com