FICO Decisions

EXECUTIVE BRIEF

FICO® Analytic Cloud Security and Compliance

The FICO® Analytic Cloud Ecosystem

The FICO® Analytic Cloud is a complete end-to-end platform and solutions ecosystem that provides access to data science tools, application development software, on-demand infrastructure, decision management applications, and packaged analytic content from FICO and trusted partners. The FICO Analytic Cloud provides a community and marketplace for analytics and decision management, and an infrastructure for the development, deployment and use of big data, advanced analytics and decision management solutions.

The flexibility and accessibility of the cloud allows people to discover new opportunities and respond to changing markets faster than ever before. Applications that used to take months or years to develop and deploy are now in users' hands in weeks. But the efficiencies of cloud computing require increased levels of trust—trust that your data is protected with the level of care that you and your customers deserve. This document provides the information you need to feel confident about the FICO® Analytic Cloud and about FICO as your cloud provider. Our goal is to deliver the peace of mind that lets you focus on using software rather than worrying about maintaining it. Our approach to servicing solutions in the FICO Analytic Cloud is keenly focused on trust and security, including:

- Secure software development
- Payment Card Industry Security Standards Council (PCI) compliance
- Tight access controls
- Detailed audit trailing
- Standards-driven operations

Security Overview

Your customer data, business data and IP are critical assets for you and your organization. In protecting these assets for you, FICO has taken a multi-faceted approach to data security that covers:

- User-specific access controls
- Access and use transparency
- Data center security
- Security for data in transit and at rest
- Redundancy
- Building secure software

We are committed to incorporating the appropriate application security controls and ensuring the confidentiality, integrity and availability of all applications we developed and/or maintain. FICO embraces PCI and Open Web Application Security Project (OWASP) standards for all development (regardless of whether the application is intended to manage or store PCI or other sensitive data). All facilities from which FICO operates FICO® Analytic Cloud solutions are built and operated to PCI standards, enabling PCI Data Security Standard (PCI-DSS) certification for those applications where it is required, and simultaneously benefitting all other solutions provided by FICO through these facilities.

FICO follows and enforces industry best practices for security and best practices in software development (please see the Secure Software Development Lifecycle section for more details). FICO conducts regular audits to check on compliance with these internal standards.

FICO continues to evolve these internal standards and best practices through alignment with standards from the Cloud Security Alliance, review of other industry guidelines, and regular independent review by third parties.

User-Specific Access Controls

Your data is **Your** Data. FICO uses your data only for the purposes you have authorized through your agreement(s) with FICO. Please see the FICO® Analytic Cloud Privacy Policy, specific license agreements you may have with FICO, and the terms and conditions for subscriptions you have made through the FICO Analytic Cloud Marketplace.

FICO lets you control access to your data in your own environment on the FICO Analytic Cloud for your registered users.

Registered users log in to the FICO Analytic Cloud through a Single Sign-On (SSO) feature that is supported by a secure identity and access management service (please see FICO Analytic Cloud Access Control section for more details).

You are able to allow or block users' access to your applications. In addition, administrators can control, from within specific applications, user functionality. **Please see the FICO Analytic Cloud website (www.ficoanalyticcloud.com) for more specifics regarding the solutions that interest you.**

Access and Use Transparency

FICO logs and safeguards audit data for at least one year and will make these reports available upon client request. The requested and protected audit reports contain data for events that include user identification, event type, date and time, success or failure indication, event origination, and identity or name of affected data, system component portal logs or resource.

FICO manages and protects user log files, and protects these files from any unauthorized modifications. FICO will:

- Back up audit trail files to a centralized log server
- Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts
- Retain audit trail history for a minimum of one year

Data Center Security

FICO has built data center environments specifically to host the FICO® Analytic Cloud and the unique security and privacy requirements of analytic customers, including clients leveraging solutions that manage personal, financial and healthcare information. The globally dispersed data center infrastructure utilizes industry best practices to minimize downtime, deliver security and protect against malware and other cyber threats. The best practices of the FICO data center environments include:

- Up-to-date physical and electronic safeguards
- Physical and electronic managed access based on the principles of need-to-know and least privilege, meaning all access must be granted in a manner that allows only the necessary rights to perform the function of the defined role
- Ongoing monitoring of internal resources with warning and critical thresholds configured to alert our 24/7 Support Team of any potential degradation or interruption of service
- A dedicated client-facing support organization focused on providing the highest levels of customer support
- Industry-standard disaster recovery capabilities
- Geographically distributed data centers
- A global support organization designed to ensure systems run effectively on a 24/7 basis

Currently, the FICO Analytic Cloud has been designed to deliver 99.9% or 99.99% uptime availability, depending on the selected solution. Service level standards (SLAs), including uptime/availability standards for individual solutions available through the FICO Analytic Cloud vary. **Please see the FICO Analytic Cloud website (www.ficoanalyticcloud.com) for more specifics regarding the solutions that interest you.**

Security for Data in Transit and at Rest

Foundational to securing your data in transit and at rest is a FICO® Analytic Cloud infrastructure that has been designed based on the concept of "Defense in Depth." We use multiple independent computer networking techniques that are mutually supporting in order to provide redundancy.

Best practices incorporated into the FICO Analytic Cloud infrastructure include:

- Demilitarized Zones for Internet facing services
- Network Monitoring/Intrusion Detection
- DdoS Network Protections
- Multiple layers of external firewalls
- PCI-DSS application-specific requirements

FICO uses the latest technology and industry best practices for encrypting data in transit and at rest. For data in transit we use current encryption protocols and hashing algorithms, encrypting data across networks with industry-standard SSL certificates. FICO uses a range of industry-standard techniques to protect sensitive data at rest, including encryption, redaction and obfuscation. Of course, the best protection against data loss is to avoid sharing or storing data beyond the level necessary to meet your business objective. FICO will work with you to understand your business requirements and ensure that those are met with the minimum amount of data movement and retention.

Products and solutions on the FICO Analytic Cloud use an encryption approach that is tailored to the specific solution. If you would like more information about data at rest encryption for any specific solution, **please refer to the solution details on the website at www.ficoanalyticcloud.com.**

The Secure Software Development Lifecycle: Building Secure Software

At FICO, software security is a method and way of building products that starts from the conception before even one line of code is written by a FICO development team. A keystone at FICO in building secure products is the Secure Software Development Lifecycle (SSDL) Program.

The SSDL program guides development teams at FICO on development practices that assure that FICO-developed products are secure, and are developed with appropriate application security controls to ensure confidentiality, integrity and availability.

SSDL training and development standards are based on a hybrid risk model guided by industry best practices based on OWASP and other industry guidelines. It also includes requirements for application design, coding and testing practices to avoid vulnerabilities and protect against common threats.

The SSDL includes:

- Computer Based Training (CBTs)
- Security (peer) Code Review
- Static Code Analysis (SCA)
- Dynamic Application Security Testing (DAST)
- Vulnerability Assessments
- Open Source Scanning

FICO® Analytic Cloud Access Control

The FICO® Analytic Cloud is supported by a set of core identity and access management services. These services regulate how people log in to the FICO Analytic Cloud and associated products through a Single Sign-On (SSO) capability. Access management includes the processes and technologies used to create, validate, protect and disable user accounts. The same login, auditing, roles and permissions are used across the entire FICO® Analytic Cloud for all products and solutions. The following techniques are used to protect access:

- Account lockout, timeout and password expiration
- Strict password strength requirements

The Cloud Security Alliance

FICO is a member of The Cloud Security Alliance. The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance for cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing (www.cloudsecurityalliance.org). The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

Compliance: Verified by Independent Third Parties

FICO follows and enforces the industry-specific standards PCI-DSS and ISO 27001. These standards are subject to independent assessment and certification that is performed by accredited third parties. A copy of these audits is available upon request.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard for all organizations that process, store, transmit and manage payment card data.

FICO has adopted PCI development standards across its software development function (i.e., for all application development work, regardless of the applications' intended use). PCI-DSS certified applications means that the solutions as delivered through the FICO® Analytic Cloud adhere to/meet all of the PCI Security Standards and have been certified as such by an independent assessment organization. For these applications, a PCI Attestation and Report of Compliance (AOC/ROC) is performed annually by an external, qualified security assessor. **If you have a question about the PCI certification of a solution offered through the FICO Analytic Cloud, please contact us.**

PCI Security Standards Council®

A Participating Organization of the PCI Security Standards Council

FICO is a participating organization of the PCI Security Standards Council and a contributor to the PCI compliance standards setting process. The Council has sought to facilitate the development of a worldwide community encompassing all areas of the payment card processing industry, in which all participants are able to review and discuss new versions of the PCI Security Standards, learn about Council initiatives, and share cross-sector experiences and best practices. **To learn more go to: www.pcisecuritystandards.org.**

ISO 27001

The FICO® Analytic Cloud is built and managed to the ISO 27001:2013 standard, which provides requirements for establishing, implementing, maintaining and continually improving an information security management system.

ISO International Organization for Standardization

About FICO

FICO (NYSE: FICO) powers decisions that help people and businesses around the world prosper. Founded in 1956 and based in Silicon Valley, the company is a pioneer in the use of predictive analytics and data science to improve operational decisions. FICO holds more than 165 US and foreign patents on technologies that increase profitability, customer satisfaction and growth for businesses in financial services, telecommunications, healthcare, retail and many other industries. Using FICO solutions, businesses in more than 100 countries do everything from protecting 2.6 billion payment cards from fraud, to helping people get credit, to ensuring that millions of airplanes and rental cars are in the right place at the right time. **Learn more at www.ficoanalyticcloud.com.**

FICO

FOR MORE INFORMATION
www.fico.com
www.fico.com/blogs

NORTH AMERICA
+1 888 342 6336
info@fico.com

LATIN AMERICA & CARIBBEAN
+55 11 5189 8267
LAC_info@fico.com

EUROPE, MIDDLE EAST & AFRICA
+44 (0) 207 940 8718
emeainfo@fico.com

ASIA PACIFIC
+65 6422 7700
infoasia@fico.com

4308EX_EN 10/16 PDF