Overview

This document provides details on how aPersona's adaptive multi-factor authentication meets U.S. regulatory compliance requirements as defined by each regulation. In addition, aPersona provides detailed risk analytic data by user and transaction for more detailed compliance reporting.

SSAE 16 [Internal Controls over Financial Reporting (ICFR)]

Statement on Standards for Attestation Engagements No. 16 (SSAE 16), is a standard used for reporting on controls at service organizations that perform critical outsourcing functions that have a true nexus and/or link with Internal Control Over Financial Reporting (ICFR). Highlights include:

"A process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

(1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant;
(2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant; and
(3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements."

http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_2_Appendix_C.aspx

aPersona's additional "layered security" factors include multiple device fingerprints, one-time use cookies, network identification, geographical information & time-based historical access of these factors. aPersona has the capabilities needed to prevent unauthorized access to controlled information and provides timely detection of fraudulent attempts to circumvent authentication.

Federal Financial Institutions Examination Council (FFIEC)

The purpose of this 2005 guidance and follow-on 2011 supplement is to provide a risk management framework for financial institutions offering Internet-based products and services to their customers. Highlights include:

- Financial institutions should review and adjust their customer authentication prior to implementing new electronic financial services, or at least every twelve months.
- Financial institutions should implement "layered security, ..consistent with the risk… for covered consumer transactions"…and "enhanced controls for system administrators". (*FFIEC Information Security Booklet*, p. 21)
- Implementation of a "Complex Device Identification" that "creates a Complex Digital Fingerprint" is preferable that "uses 'one-time' cookies and looks at a number of characteristics including PC configuration, Internet protocol address, geo-location, and other factors.

http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20%28FFIEC%20Formated%29.pdf

aPersona's additional "layered security" factors include multiple device fingerprints, one-time use cookies, network identification, geographical information & time-based historical access of these factors. aPersona transaction verifications can be executed any time with different security profiles "layered in" that are "consistent with the risk" of transactions. aPersona can be used to satisfy the multi-factor authentication guidance set forth by FFIEC.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA require that national standards for electronic health care transactions be established. The Technical Safeguards section requires covered entities to control access to computer systems and to protect communications containing Electronic Protected Health Information (EPHI) transmitted electronically over open networks (i.e. remote access) from being intercepted by anyone other than the intended recipient. Highlights include:

"Security Rule" of HIPAA by providing "appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information".

Implement two-factor authentication for granting remote access to systems that contain EPHI. This process requires factors beyond general usernames and passwords to gain access to systems.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

aPersona's additional factors "beyond general usernames and passwords" include multiple device fingerprints, network identification, geographical information & time-based historical access of these factors which can be used to satisfy HIPPA two-factor authentication.

Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. Highlights include:

PCI guidelines requiring organizations to "Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service or terminal access controller access control system with tokens; or virtual private network with individual certificates."

https://www.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf

aPersona's additional authentication factors include multiple device fingerprints, one-time use cookies, network identification, geographical information & time-based historical access of these factors. aPersona enables two-factor authentication capabilities to validate the identity of a user prior to authorizing access to sensitive information such as cardholder data.

Criminal Justice Information System (CJIS) Security Policy

CJIS provides state, local, and federal law enforcement and criminal justice agencies with access to centralized information such as fingerprint records, criminal histories, and sex offender registrations. The CJIS Security Policy sets forth the minimum requirements for securing access to CJIS data and information. Highlights include:

Utilizes two of the acceptable methods specifically identified in section 7.3.2.3.1 "Definitions and Policies for Advanced Authentication". Virtual Token® MFA combines "public key infrastructure (PKI)" with "software tokens".

Access to certain CJIS data systems may require "Level 3" authentication. Virtual Token® MFA validates a "soft crypto token" (Level 3) against a digital signature retrieved from the user's physical device (a "hard crypto token" = level 4). Virtual Token® MFA therefore validates at between Level 3 and Level 4.

http://www.imprivata.com/sites/default/files/cjis_compliance_wp__1_.pdf (See Page 2)

CJIS Advanced Authentication Requirements:

What is Advanced Authentication?

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure

(PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification

aPersona's additional advanced authentication factors include multiple device fingerprints, one-time use cookies, network identification, geographical information & time-based historical access of these factors. aPersona transaction verifications can be executed any time with different security profiles that enable true "Risk-based Authentication. aPersona can be used to satisfy the "advanced authentication" guidance set forth by CJIS.

National Institute of Standards and Technolgy (NIST)

NIST 800-63-1 Electronic Authentication Guidelines provide technical recommendations for remote electronic authentication to the Federal IT system.

The Office of Management and Budget (OMB) guidance, E-Authentication Guidance for Federal Agencies, [OMB 04-04] list four levels of authentication. NIST 800-63-1 provides requirements for each.

- Level 1 Little or no confidence in the asserted identity's validity.
  - No identity proofing is required at this level, and simple password challenge-response protocols are allowed.
- Level 2 Some confidence in the asserted identity's validity.
  - A single authentication factor is required. This must be something you know OR something you have.
- Level 3 High confidence in the asserted identity's validity.
  - A minimum of two authentication factors is required. This must be something you know PLUS something you have.
- Level 4 Very high confidence in the asserted identity's validity.
  - This level is similar to Level 3 except that only "hard" cryptographic tokens are allowed

http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

aPersona's additional advanced authentication factors include multiple device fingerprints, one-time use cookies, network identification, geographical information & time-based historical access of these factors. aPersona address the requirement for NIST Level 3 Assurance when an existing password authentication.

FIPS-180-4
Hash Compliance: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

> This Standard specifies secure hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 - for computing a condensed representation of electronic data (message).

aPersona utilizes SHA1 hash algorithms as set forth in the NIST FIFS Pub 180-4.

FIPS200 Compliance

Minimum Security Controls: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

To meet "appropriate security controls" defined by FIPS200, Virtual Token® MFA combines passwords and tokens as specified in NIST Special Publication 800-53. The password is validated by the organization when it validates its user's login ID and password. The token number is then produced for the user's device, entered by the user (or auto-entered by the process) and then validated against the user's device by the Virtual Token® engine.

aPersona creates one-time use passcodes (or tokens) that are validated against the user's device, network and geography and must be entered by the user.

NIST 800-3 Recommended Security Controls:

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

- An information system can employ security controls at different layers within the system. An operating system, for example, typically provides an access control capability that includes the identification and authentication of users. An application, hosted by that operating system, may also provide its own access control capability requiring users to go through a second level of identification and authentication, thus rendering an additional level of protection for the information system. Organizations carrying out the security control selection process consider components at all layers within the information system as part of effective organizational security architecture implementing a defense-in-depth security strategy.
- Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

aPersona's additional advanced authentication factors include multiple device fingerprints, one-time use cookies, network identification, geographical information & time-based historical access of these factors. aPersona's unique federated Multi-Factor technology enables centralized control of multi-factors across multiple applications and layers of access within an organization supporting a "defense-in-depth security strategy".

