MAY 2023

BIOMETRICS, MULTI-FACTOR AUTHENTICATION, AND CYBER LIABILITY INSURANCE

PATRICK SICKELS
INTERNAL AUDITOR
CU*ANSWERS

CONVERSATIONS ON COMPLIANCE

CU*ANSWERS
A Credit Union Service Organization

SPEAKER

Patrick Sickels began his career as an attorney, and quickly branched out into the technological services industry, where he used his legal skills to help companies manage their compliance requirements.

Patrick used these skills to develop into a certified auditor and risk manager.

DISCLAIMER #1. CU*Answers does not provide legal advice and cannot provide an opinion as to whether the risks identified in this document applies to your organization in the jurisdiction(s) where you do business. If you have concerns whether you are at risk of regulatory action or lawsuit, CU*Answers recommends you provide your own legal counsel with information regarding your current security practices and disclosures.

DISCLAIMER #2. Although CU*Answers may use and resell third-party products discussed in the document, CU*Answers cannot warrant such products will be suitable for your organization. Any such warranties will be described in the contracts for any such third-party product or service.

AGENDA

KEY ITEMS

Agenda

BIOMETRICS
Biometrics are increasingly important in authentication today. What are the risks and rewards? How should you prepare?

MFA
Multi-factor authentication needs to be addressed by financial institutions. What are the important considerations?

CYBER LIABILITY INSURANCE
Cyber liability insurance is maturing and adapting. What should you know about the latest trends?

BIOMETRICS

Defining Biometrics

There is no absolute clear legal definition on what constitutes "biometric data" that must be protected. What we have is a general consensus.

BIOMETRIC INFORMATION

The trigger for review is **any data** that measures a person's unique physical characteristics, including but not limited to fingerprints, palmprints, voiceprints, facial, retinal, or iris measurements, **that can be used to identify a unique individual**.

EXCLUSIONS

Exclusions include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, and physical descriptions such as height, weight, hair color, or eye color. Capturing a driver's license would **not** be considered "biometric" although the license would still need to be transmitted and stored securely due to other laws protecting consumer information.

Biometric Example

Where a selfie is compared against a driver's license, the facial data used to identify a person from the ID is considered biometric data.

SELFIE (FACIAL MEASURMENTS)
The selfie photo takes facial measurements and uses an algorithm to determine the probability that the person taking the selfie is the same in the ID photograph. This data is **biometric**.

DRIVERS LICENSE
The driver's license is used by the algorithm as the base to compare the probability as to whether the person in the selfie is the same as the person in the ID. The license itself is **not biometric** (although must be transmitted and stored security based on privacy laws).

ADVANTAGES

Why Biometrics?

Biometric use is **accelerating in the fintech space**. Even if your institution has no interest in biometrics, you may run across biometrics in the third-party services offered to members and consumers.

RISK REDUCTION

Biometric data helps reduce the risk of fraud-based crimes such as identity theft or money laundering. Biometrics are also ideal for protecting sensitive financial transactions.

COST

Biometric data is usually cheaper to store and use than other forms of multi-factor authentication. For example, biometric can be both instantaneous for the user and less expensive to the organization than sending a text message.

STATE LAWS

Risks: State Laws

Three states directly address biometric protection requirements: **Illinois, Texas, and Washington**. However, six other states have privacy laws that likely encompass biometric data.

ILLINOIS
Biometric Information Privacy Act ("BIPA") 740 ILCS 14/1 et seq. BIOMETRIC SPECIFIC. Depending on whether a private entity is possessing, capturing, collecting, otherwise obtaining, or disclosing biometric information or biometric identifiers, requires: (1) a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information; (2) compliance with that policy; (3) protection of the biometric information using the reasonable standard of care within the industry or in a manner as protective as the entity protects other confidential and sensitive information; (4) informing the subject whose biometric information is to be collected of the specific purposes and length of term for which biometric information is being collected, stored, or used; and (5) receiving a written release from the individual to proceed with the collection or disclosure of the biometric information.

CLASS ACTION? Yes, provides for recovery of liquidated statutory damages or actual damages, and attorneys' fees and expenses.

TEXAS
Texas Capture or Use of Biometric Identifier Act ("CUBI") TEX. BUS. & COM. CODE ANN. § 503.001. BIOMETRIC SPECIFIC. Requires that a person capturing a biometric identifier of an individual for a commercial purpose inform the individual before capturing the biometric identifier and receive the individual's consent and requires protecting the data from disclosure using reasonable care and in a manner as protective as the entity protects other confidential information. Biometric identifiers must be destroyed within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the biometric identifier expires. Also prohibits a person in possession of a biometric identifier of an individual from selling, leasing, or otherwise disclosing the biometric identifier unless in certain circumstances.

CLASS ACTION? No, provides for a civil penalty of no more than $25,000 for each violation, enforceable by the Texas Attorney General.

Risks: Other Laws

Non-specific data privacy state statutes* could be used as the basis of lawsuits against fintech companies and financial institutions for improper use and storage of biometric data.

CALIFORNIA
California Consumer Privacy Act ("CCPA"). Comprehensive data privacy statute that includes obligation to make certain disclosures regarding collection of biometric data.

CLASS ACTION? Yes, where the information was involved in an unauthorized exposure as a result of the business' failure to implement and maintain reasonable security procedures and the business' failure to take certain steps after receiving a consumer request.

MARYLAND
Personal Information Protection Act ("PIPA") MD. CODE ANN., COM. LAW §§ 14- 3501 et seq. Requires a business to take reasonable steps to protect against unauthorized access to or use of personal information (including biometric data), including requiring in contracts with certain nonaffiliated third-party service providers that the service provider will implement and maintain reasonable security procedures and practices.

CLASS ACTION? Yes, where individuals can sue to recover their injuries or losses as a result of violations of the Maryland Act.

*Arkansas, California, Colorado, Maryland, New York, and Virginia.

Lawsuits

Very different states with very different politics still place organizations at risk for the misuse or loss of biometric data. Even without a specific statute, every organization could still be sued under a **negligence theory**.

LAWSUITS

ILLINOIS

An Illinois jury found a company violated the Illinois Biometric Information Privacy Act ("BIPA") 45,600 times over six years by collecting truck drivers' fingerprints to verify identities without informed, written consent. The case was a class action lawsuit and the first jury verdict rendered under BIPA. **The federal judge assigned to the case awarded the plaintiff-class a judgment totaling $228 million**. Given the size of the verdict, this case will almost certainly be appealed or settled.

TEXAS

The Attorney General is suing Google based on an alleged failure to (1) to obtain informed consent from Texas citizens regarding the use of facial and voice biometric information through Google's applications, and (2) failure to delete the biometric information in a reasonable time. Texas is one of the states that regulates the capture, use, and disposal of biometric information, and this is the first lawsuit against a company under this law. **Google faces civil penalties of up to $25,000 per violation**.

LAWSUITS

Strict Liability

Biometric laws tend to be strict liability, meaning **mistake is not a defense**. The only item that matters is whether the statute was violated or not. "Willful" violations are only used to assess damages, and lack of willfull violations is **no defense**.

You may have noticed that in neither the Illinois or Texas lawsuits is there any allegation that the persons had their data stolen or even suffered any loss whatsoever. Plaintiffs or the attorney generals do not need to prove that there were losses as a result of a statutory violation. **Mere violation of the statute is enough for there to be damages against the violator**.

These laws are **do the crime, pay the fine**.

WHAT TO KNOW

Key Elements

Before launching a biometric project, there are a few items that your organization should understand thoroughly before providing to your consumers.

1

WRITTEN POLICY
The entity acquiring the biometric information must have a publicly available written policy, including:

What the data is used for;
Retention period of the data;
Destruction of the data; and
The rights of the consumer, including the right to request data is destroyed.

2

CONSENT
The entity acquiring the biometric information must receive from the consumer written and informed consent. This consent should:

Include acknowledgement that the privacy policy was made available; and

Provide a record that the consent was made.

3

NO COMMERCIAL USE
Biometric information is not used for any other commercial purpose (sold, leased, traded, or profited from).

4

NO DISCLOSURE
Biometric information may not be disclosed or disseminated, except for the purpose for which the information was obtained.

5

SECURITY
Some level of commercially reasonable security based on the sensitivity of the data (appropriate industry-standard encryption in the transmission and storage of biometric data).

SDLC

CU*Answers Response

SDLC UPDATE

To protect the organization, CU*Answers has amended the Software Development Life Cycle (SDLC) policy to make sure the key risks are addressed.

Privacy Policy	Consent	Secure Acquisition	Secure Transmission	Secure Storage	Destruction	Third Parties
The client has a publicly available Privacy Policy that states what the biometric data is used for, its retention, destruction, and the rights of the consumer.	The client obtains consent from the consumer to acquire the biometric data.	The site or application that acquires the biometric data does so with security standards consistent with this SDLC.	The biometric data is transmitted using security standards consistent with this SDLC.	The biometric data is stored according to security standards consistent with this SDLC.	Biometric data is destroyed as soon as it has fulfilled its purpose, or shortly thereafter if maintained for troubleshooting or other reasonable purposes, consistent with other security standards in this SDLC.	Biometric data is not provided to third parties unless these parties are needed for the service and have agreed to indemnify CU*Answers.

MULTI-FACTOR AUTHENTICATION

MFA

Rise of MFA

Multi-Factor Authentication (MFA) is rapidly becoming the new "encryption." Eventually, you will be considered to not have "commercially reasonable security" without MFA.

STATUTORY

The new FTC Safeguards Rule requirement is for financial institutions must implement MFA for anyone accessing customer information. The FTC rule on MFA must be in place by June 9, 2023.

Multi-Factor Authentication (MFA) must use at least two of the following three factors:

Knowledge Factor (something you know, e.g., a password)

Possession Factor (something you have, e.g., a security key)

Inherence Factor (something you are, e.g., a fingerprint)

INSURANCE

MFA has now become a cyber-insurance requirement by most insurance agencies to qualify for coverage.

The primary requirements for cyber insurance providers for MFA:

Business email access

Remote employees

Administrative access

DUO

Cisco Duo

MFA IS IN PRODUCTION AT CU*ANSWERS

CU*Answers implemented MFA on desktops and laptops for administrator access using Cisco Duo. The implementation went well and met all of the requirements for our cyber insurance carrier. CU*Answers has a plan to migrate all staff to MFA.

MFA was already in production for VPN access.

CONSIDERATIONS

MFA Considerations

Your most important considerations are whether the solution is **compliant** and meets **insurance requirements**. However, there are also significant other issues that need to be considered before deciding on a solution.

IMPLEMENTATION

Cost – what is the cost of the license and how often will the provider have the ability to raise costs?

Training and Onboarding - how much training will be needed for both end users and support staff?

Options – what about staff without cell phones? Will tokens be deployed?

ADMINISTRATION

Support – end user experience will be inherently negative; how much additional time will it take support staff to respond to authentication issues? How often do users sign in?

Enhancements and Upgrades – enhancements and upgrades will disrupt the organization and will need planning and rollback procedures.

IT'S ME 247

Online Banking

CU*ANSWERS IS EVALUATING MFA SOLUTIONS FOR ONLINE AND MOBILE BANKING

CU*Answers is looking at options for providing MFA solutions for Online and Mobile Banking products. We have completed a couple of projects that implement MFA, such as an option to require MFA when a member changes their personal information.

Some of the considerations for MFA include:

- What to do for joint accounts?
- What solution? Text messages will be expensive!
- Accurate email and cell phone information is imperative, or your members and consumers will have a very bad experience.

MFA ISSUES

MFA Vulnerabilities

Although MFA is effective, this solution is not bulletproof. Attackers have already figured out methods to defeat MFA. These methods need to be known to users and support staff as part of implementation and retraining.

1

MFA FATIGUE

Malicious hackers bombard victims with 2FA push notifications to trick them into authenticating their login attempts. This has been successfully used against Office 365 users. The victims approve similar notifications all the time, and due to the notification overload to spot the threat.

2

SESSION HIJACKING

User is tricked into visiting a malicious web site. User provided credentials, presented to the legitimate site. Legitimate web site sent back legitimate session token stolen by the attacker.
hijacking, even if 2FA is involved

3

DUPLICATE CODE

Most random number generators start with a randomly generated seed value, which is used to generate the first value. Attackers that learn seed number and algorithm can generate duplicate or identical code generators that match the victim's code.

CYBER LIABILITY INSURANCE

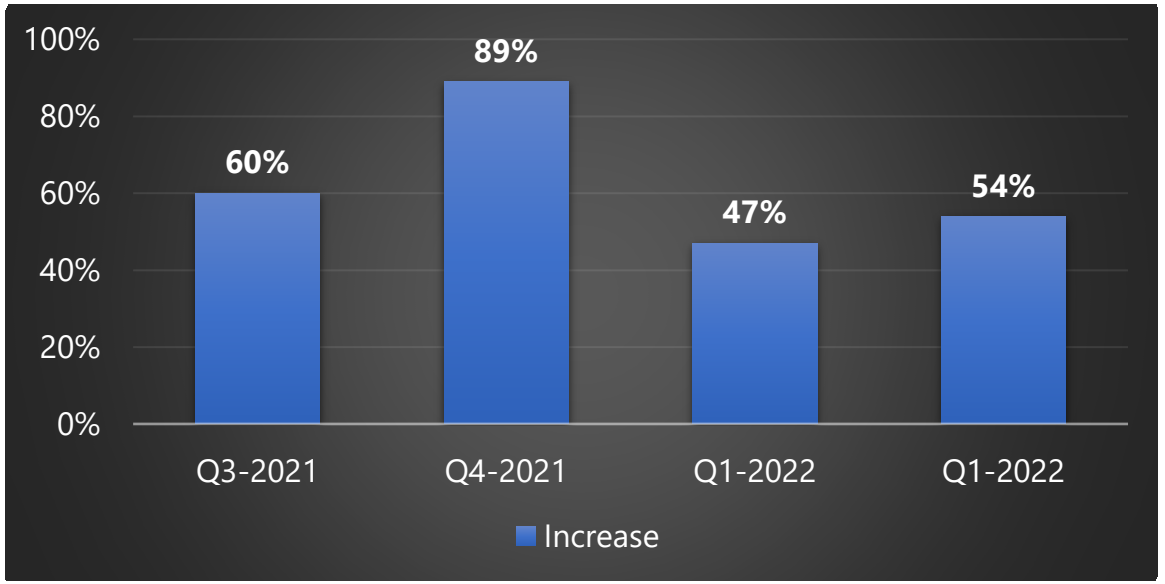
INSURANCE

Cyber Liability

The cyber insurance market has started to stabilize after years of steep rate increases. Rate increases were driven by ransomware claims, especially through and business email compromises and funds transfer schemes.

DENIAL OF QUOTES AND COVERAGE

The heavy losses incurred by insurance carriers have prompted more frequent denials of coverage or even quotes to organizations that do not meet certain requirements.



https://www.risk-strategies.com/

MFA ITEMS

MFA and Insurance

CU*Answers' insurance carrier provided guidance on what would be and "acceptable" MFA implementation at CU*Answers. Sharing this information but your milage may vary.

MFA REQUIREMENTS

- "Conditional" or "Adaptive" access should not limit the frequency of an MFA challenge to more than every 24 hours.
- All service accounts must have interactive login disabled. Service accounts with interactive login disabled do not require MFA.
- A user or device certificate when combined with an MFA challenge is valid, however a user or device certificate by itself is not considered valid MFA.
- MFA requirement applies to both internal (on premise) and remote access.

MFA ITEMS

Email and Insurance

MFA is normally required unless an on-premises email server without web access is in place.

SERVICE	DESCRIPTION	INTERNET FACING	MFA REQUIRED	SUGGESTED ACTION
EMAIL	Email SaaS Platform(s) O365/Google	YES	YES	Cloud/Internet facing email services must utilize MFA. (Office 365/Exchange On-Line (EOL), Google Workspace, Yahoo, etc.) Most of the bigger SaaS services/platforms have MFA built into them. It only requires turning the features on and training users.
	Email services Web-hosted/Internet Service Provider (ISP)	YES	YES	Hosted/ISP email services by default are internet-facing and require a second factor beyond username/password. (Rackspace, Comcast, Verizon, etc.) Most have the ability to enable MFA. If not, it might require migrating to a more secure platform.
	Email Servers On-Premises	PARTIAL	YES – WHEN WEB ACCESS IS ALLOWED	On-Premises email servers that are 100% behind your organizations firewall DO NOT require MFA. (Exchange, Lotus Notes, Postfix, Zimbra, etc.) However, if you allow web access such as MS Exchange Outlook Web Access (OWA) or Mobile Devices to access email such as MS ActiveSync then MFA and other Mobile Device Management (MDM) protections should be in place.

REMOTE ACCESS

Remote Access

VPN and remote desktop tools require MFA. Administrative rights to certain systems requires MFA.

SERVICE	DESCRIPTION	INTERNET FACING	MFA REQUIRED	SUGGESTED ACTION
REMOTE ACCESS	Virtual Private Network (VPN) Access	YES	YES	To enhance security on VPNs, utilize additional factors beyond username/passwords. VPN is a secure encrypted gateway/pathway directly into your organization's on-premise network from outside.
	Remote Desktop support tools	YES	YES	Remote Desktop tools (LogMeIn, Splashtop, GoToMyPC, Teamviewer, etc.) should all have MFA enabled on their management portals. These tools provide remote access directly into your organization's on-premises network by allowing direct access to Servers/Desktops/Laptops/VMs.
	Managed Service Providers (MSPs) use Remote Management & Monitoring (RMM) tools	YES	YES	MSPs use RMM tools (ConnectWise, NinjaRMM, Kaseya, Atera, MS Intune, etc.) which should have MFA enabled. These tools provide third-party MSPs access directly into your organization's network. Specifically, they can get onto Servers/Desktops/Laptops/Virtual Machines/Network Equipment, etc. These RMM tools are secure and encrypted but should require MFA to gain access.
	Virtual and Application Gateways	YES	YES	Virtual gateways like VMWare's Horizon, Citrix Virtual gateways or other MFA/IdP (Identity Provider) application gateways that allow direct access from the internet to virtual machines or applications inside your network should all require MFA. These solutions are internet facing and therefore require MFA.

DIRECTORY

Directory Access

Domain Admins and management consoles for backups should have MFA enabled.

SERVICE	DESCRIPTION	INTERNET FACING	MFA REQUIRED	SUGGESTED ACTION
DIRECTORY SERVICES	Microsoft Active Directory, LDAP	NO	YES	Requiring that Domain Admin level credentials are challenged with MFA makes it much harder for nefarious actors to easily gain privileged access on your systems and network. Additionally, challenging Identity internally helps restrict bad actors from stealing elevated credentials, executing ransomware payloads and makes lateral movement much more difficult.
BACKUPS	Backup software management	NO	YES	The management console of your backups should be protected with MFA. (Veeam, Datto, Veritas, Barracuda Backup, etc.) Your backups should be protected in transport using encrypted transport protocols; you also need to ensure that your backups are stored securely using either encryption, strict Role-Based Access Controls (RBAC) or airgap measures. The final step is using MFA to protect the management console.

INFRASTRUCTURE

Network Infrastructure

Management consoles of network equipment and local/domain level administrator access also require MFA.

SERVICE	DESCRIPTION	INTERNET FACING	MFA REQUIRED	SUGGESTED ACTION
NETWORK INFRASTRUCTURE	Firewall, Router, Switch, Hub and Wireless Access Point Management	NO	YES	The management console of network equipment should be protected with MFA. There are several ways to protect access. First, all the MFA/IdP providers use an Authentication RADIUS Proxy. Any system that is RADIUS Authentication capable can be paired up with an Auth Proxy. Many Firewall/Router/Switch brands have the built-in ability to turn on a second factor as well. Lastly, using/creating a management network by segmentation/IP restrictions and using an access gateway protected with MFA is acceptable architecture, too.
ENPOINTS	Servers, Desktops, Laptops, Virtual Machines	NO	YES	All local and domain level administrator access to endpoints should be protected with MFA. (Cisco Duo, OKTA, OneLogin, Ping, WatchGuard, AuthLite, UserLock, etc.) Most MFA/IdP providers have operating system clients that when coupled with LDAP synchronization and an Identity Portal allow for MFA challenges when logging into endpoints with elevated accounts.

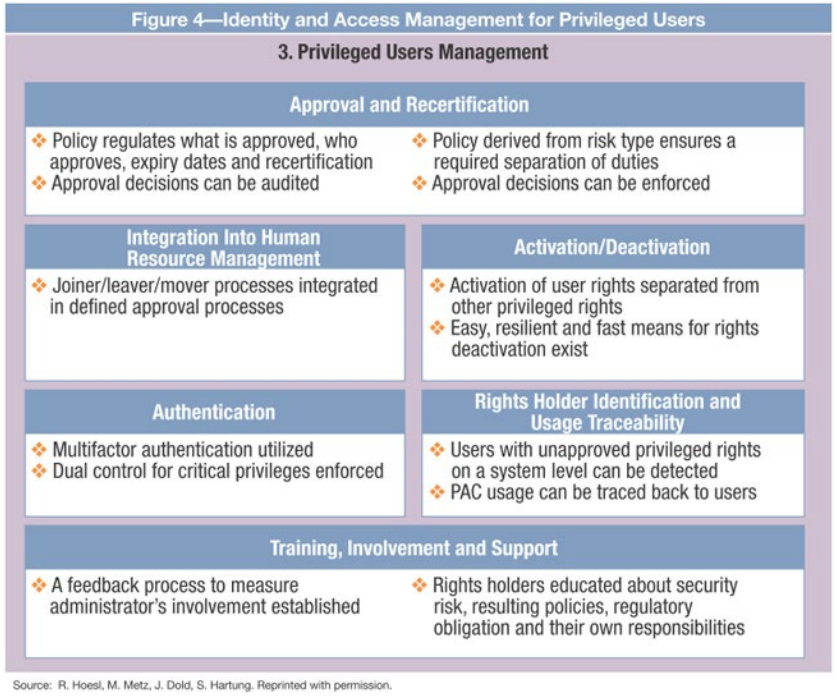
PAM

PAM

PRIVILEGED ACCESS MANAGEMENT

Insurers are increasingly interested in whether the organization has Privileged Access Management ("PAM") over the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment.

The central goal is the enforcement of least privilege, defined as the restriction of access rights and permissions to the absolute minimum necessary to perform routine, authorized activities.



https://isaca.org

PAM GENERAL REQUIREMENTS

A clearly defined process specifying how roles and rights have to be requested, providing rules for expiry dates, and enabling recertification and on-demand auditing.

Integration into human resource management and activation/deactivation.

Authentication and rights holder identification and usage traceability to highly critical privileges.

The automated ability to trace back privileged activities to personal identities and to detect illicitly assigned privileges.

Active support and training of responsible persons and users.

WHAT TO KNOW

Additional Items

Although MFA is the largest item of focus for cyber liability insurers, there are other items that should be addressed to mitigate risk and control premiums.

1

ENDPOINTS
Control endpoint devices security whenever possible, especially with Internet of Things (IoT) devices that may not have adequate security upon installation. Ensure items such as fire alarms that are connected to the network are secure.

2

SaaS
Ensure the organization has a plan in case there is a breach at a SaaS provider. Avoid sending member data to third-parties that is unnecessary for the services.

3

TRAINING PROGRAMS
Enhance training programs and consider having social engineering testing for employees. Document the findings and work on remediation where needed.

4

EMPLOYEE DISRUPTIONS
As retaining employees becomes more volatile, ensure that regular access reviews are documented.

5

DISASTER RECOVERY
Don't lose focus on disaster recovery, and ensure the plan encompasses remediation for a cyberattack, especially ransomware.

EXCLUSIONS

Insurance Best Practices

As with any insurance policy, your organization should be up to speed on exclusions, and to have a plan if insurance is denied based on these exclusions. Additional coverage may be possible to cover some of these gaps.

- **Prior Knowledge Exclusion**. Coverage will not apply to incidents that were known or reasonably foreseeable by the insured prior to the policy's inception.
- **Wear and Tear Exclusion**. Wear and tear exclusions typically apply to physical components of a computer system, such as hardware or storage devices, which may fail over time. A hardware failure could lead to data breaches or other cyber-related losses.
- **Unencrypted Data Exclusion**. If a data breach involves unencrypted data, your insurer may deny the claim based on this exclusion.
- **Contractual Liability Exclusion**. Contractual liability exclusions may limit or exclude coverage for losses arising from your business's contractual obligations, such as indemnity clauses in contracts with vendors or clients.

QUESTIONS?

CU*ANSWERS
A Credit Union Service Organization