FCI

USER SECURITY

USER SECURITY

Every identity verified, every login logged, every access decision enforced — not optional, not risk-based.

Phishing-resistant MFA, federated identity, single sign-on, cloud access security, and complete authentication logging — applied to every user across your distributed environment. From onboarding to offboarding, no gaps in between.

40,000+	400+	30+
users under management	financial services environments	years serving financial services

THE MFA REALITY

Not all MFA is created equal — and the wrong kind creates a false sense of security.

Most firms believe they are protected because they "have MFA." But MFA is not a single technology — it is a spectrum, and most of what firms deploy today is vulnerable to the exact attacks regulators are warning about.

The Push Notification Problem

Standard MFA sends a push notification to the user's phone. The user taps "Approve" and they're in. In an MFA fatigue attack, an attacker who already has stolen credentials floods the user with repeated push notifications — at 2 AM, during meetings, over and over. The user taps "Approve" just to make it stop. This caused the Uber breach (2022) and attacks on Cisco, Okta, and others.

> **THE CORE VULNERABILITY**
> Standard push-notification MFA lets a user approve an authentication request they did not initiate. One tap of "Approve" — whether intentional or out of fatigue — grants full access.

Why CISA Requires Phishing-Resistant MFA

CISA does not consider push notifications, SMS codes, or standard OTP to be phishing-resistant. In its Zero Trust guidance (OMB M-22-09), CISA mandates phishing-resistant authentication and identifies FIDO2/WebAuthn as the standard. Phishing-resistant MFA requires a cryptographic handshake that cannot be intercepted, socially engineered, or replayed.

What Phishing-Resistant MFA Looks Like

Number matching: the user sees a number on the login screen and must type that exact number into the authenticator app. Biometric re-authentication confirms the person. Two extra seconds. The user cannot accidentally approve a request they did not initiate. It stops the entire category of fatigue attacks.

AUTHENTICATION INDEPENDENCE

When the lock and the key are made by the same company under attack, you have a single point of failure.

Most firms use Microsoft Authenticator to protect Microsoft 365. But this creates a dangerous concentration of risk. If Microsoft's authentication infrastructure is compromised, the tool you depend on to verify identity is compromised at the same time.

31%	146%	50%+
of M365 breaches from token theft (2025)	rise in AiTM attacks (2024)	AiTM campaign success rate (2025)

The Token Theft Problem

In an Adversary-in-the-Middle (AiTM) attack, the attacker proxies the real Microsoft login page. The user completes MFA normally — but the attacker captures the session token. Access to Outlook, OneDrive, Teams, and SharePoint without another MFA prompt.

The AuthQuake Vulnerability (Dec 2024)

Oasis Security disclosed a critical flaw: unlimited brute-force of MFA codes with no rate limiting and no user notification. 50%+ bypass success in under 70 minutes. 400M+ Office 365 seats affected. The user never knew it was happening.

FCI's Approach: Divide to Better Secure

FCI deploys a separate, independent authentication provider outside the Microsoft ecosystem. The MFA challenge, verification, and logging happen through a different security boundary. A Microsoft compromise does not compromise the authenticator.

THE PROBLEM

Most firms cannot prove who accessed what, when, or how.

Regulators require that firms control who has access, verify identities, and log every authentication event. Most firms believe they have this covered because they turned on MFA. The reality: MFA is often risk-based, federation and SSO are misconfigured, and authentication logs are incomplete.

MFA Not Actually Enforced

Most firms enable MFA as risk-based — Microsoft decides when to challenge. If the login looks "normal," MFA is skipped. No log shows when it was bypassed.

Federation, SSO & MFA Conflated

Three different technologies. Most firms and IT providers conflate them. Misconfigured identity infrastructure creates gaps no one recognizes.

Incomplete Auth Logging

Native logs miss risk level, device location, auth method, source country. Without extended logging, firms cannot answer regulator questions.

No Lifecycle Visibility

Who tracks inactive accounts? Who detects anomalous behavior? Who ensures every access point is closed when someone leaves?

THE QUESTION EVERY FIRM SHOULD ASK

Can you prove — for every user, every login, every application — who accessed it, when, how they were authenticated, and whether the access was appropriate?

WHAT FCI DELIVERS

Six capabilities — applied to every user, enforced continuously.

FCI builds a complete authentication ecosystem — federation, SSO, CASB, and phishing-resistant MFA working together — so every access decision is verified, logged, and provable.

01
Phishing-Resistant MFA

CISA-recommended, enforced on every login. Number matching + biometric verification. Not risk-based, not optional. Every login verified.

02
Federation & Identity Sync

Centrally managed credentials synced across all integrated applications. "Log in with Microsoft" is federation — FCI configures and manages it.

03
Single Sign-On (SSO)

Different from federation. Eliminates repeated authentication within a session. Security and usability work together.

04
CASB

User verified, device trusted, network known — before access is granted. Zero Trust verification chain on every access attempt.

05
Extended Auth Logging

Full context: login time, result, user, application, risk level, device location, auth method, source country.

06
User Lifecycle Management

CISO-approved onboarding, inactive user detection, anomaly monitoring, complete decommissioning. Every change logged.

LOGIN TIME | RESULT | USER | APPLICATION | RISK LEVEL | DEVICE LOCATION | AUTH METHOD | SOURCE COUNTRY

MOBILE DEVICES

Securing mobile access without invasive MDM.

Traditional MDM drains battery, restricts users, and feels like surveillance on a personal device. FCI enforces security at the point of access instead: OS current, screen lock enabled, no jailbreak — the user remediates on their own terms. No agent. No surveillance. The firm gets security; the user keeps privacy.

HOW FCI IS DIFFERENT

Four reasons the same tools produce different results.

Every MSP can turn on MFA. The difference is mastery, automation, consistency, and persistent proof.

WHAT SETS FCI APART

Enabling MFA is not identity security. Configuring federation is not enforcement. FCI delivers both.

Expert Mastery

Hundreds of federation, CASB, and MFA deployments across financial services. FCI knows which CASB policies matter for compliance.

Automated Procedures

User provisioning, deprovisioning, and policy enforcement through templates. Identity controls enforced continuously.

Consistent Controls

Every user, every app, every login. Contractors, employees, BYOD — same standard. No exceptions.

Persistent Proof

Extended logging captures risk level, source country, device location, method. Evidence every day, not just audit day.

INTERCONNECTION

User security gates access to everything else.

A verified identity determines whether a user reaches the endpoint, the network, the data, and the cloud applications. Every domain protects every other domain.

Endpoint Security

Authentication verifies user and device before granting access

Network Security

Valid identity + unknown network triggers additional scrutiny

Cloud App Security

CASB policies tie directly to verified user identity

Data Security

User permissions anchor classification and DLP controls

Firm Security

Every auth event feeds the CISO Portal

The Principle

No single domain failure defeats the system

WHAT YOU CAN PROVE

Evidence that builds itself — every day, not just on audit day.

Regulators, home offices, and cyber insurance carriers ask: can you prove who has access? FCI produces continuous evidence as a byproduct of how it operates.

Authentication Verified

Every login verified by phishing-resistant MFA with full context

Access Controlled

CASB Zero Trust: user verified, device trusted, network known

Lifecycle Managed

CISO-approved onboarding, anomaly detection, complete decommissioning

Compliance Documented

Extended logs: who, what, when, where, how — beyond Microsoft limits

Independence Proven

Authenticator outside Microsoft — separate verification boundary

CISO Portal Visibility

Login patterns, anomalies, lifecycle changes — real-time

FINRA · SEC · NAIC · STATE REGULATORS · CYBER INSURANCE · HOME OFFICE

Ready to close the identity gaps your firm can't see?

FCI implements the authentication ecosystem that most firms think they already have — and produces the evidence to prove it.

PHONE
973-227-8878

WEB
fcicyber.com