Capital Investment Club

Security Evidence Screenshot Pack

Redacted screenshot evidence inventory for consumer MFA before Plaid Link, critical-system MFA, and endpoint detection and response tooling.

Last updated: 06/08/2026

Purpose

This evidence pack documents the screenshot evidence CIC maintains for high-risk security controls that cannot safely expose raw administrative console details on a public page.

The public pack intentionally presents redacted evidence references and control descriptions. Full-resolution screenshots, audit exports, and tool-console captures must be retained in CIC's restricted evidence repository and produced only for authorized diligence, audit, or provider review.

Evidence Inventory

Evidence item	Public evidence status	Restricted evidence retained	Review cadence
Consumer MFA implementation before Plaid Link is surfaced	Redacted evidence reference published	Yes	Before every Plaid Link production launch or material auth change
Critical-system MFA implementation for systems storing or processing consumer financial data	Redacted evidence reference published	Yes	Quarterly and after critical-system access changes
Endpoint detection and response tooling on endpoints	Redacted evidence reference published	Yes	Quarterly and after endpoint-management changes

Consumer MFA Before Plaid Link

The consumer MFA evidence screenshot must show the user-facing verification step that appears before Plaid Link or any bank-account connection flow is available.

The retained restricted screenshot should show:

- The CIC page or modal requiring verification.
- The available MFA channel or verification prompt.
- The blocked Plaid Link action state before successful verification.
- Date of capture.
- Environment or release identifier.

Public redaction must remove OTP values, phone numbers, email addresses, user IDs, session tokens, and any

bank-provider secrets.

Critical-System MFA

Critical-system MFA evidence must show that administrative access to systems storing or processing consumer financial data requires multi-factor authentication.

Critical systems include:

- CIC production cloud consoles.
- Database or storage consoles.
- Payment, wallet, banking, Plaid, Mono, Stripe, Paystack, and provider dashboards.
- Source control and CI/CD environments that can deploy or access production secrets.
- Monitoring, logging, notification, and support tools that expose consumer financial data or operational secrets.

The retained restricted screenshot should show MFA enforced for access, the tool or system class, and the review date. Public redaction must remove tenant IDs, account IDs, recovery codes, phone numbers, emails, secret names, and provider-specific tokens.

Endpoint Detection And Response

Endpoint detection and response evidence must show that CIC-managed employee or contractor endpoints have security monitoring coverage appropriate for their access level.

The retained restricted screenshot should show:

- Endpoint protection or EDR dashboard coverage.
- Device inventory or agent health state.
- Last check-in or policy status.
- Alert or monitoring capability.
- Date of capture.

Public redaction must remove device serial numbers, employee names, local usernames, IP addresses, file paths, and any security-tool tenant identifiers.

Evidence Handling Rules

- Keep raw evidence in a restricted repository or evidence vault with access limited to authorized security, leadership, and compliance reviewers.
- Keep public evidence redacted and high level.
- Record who captured the evidence, when it was captured, what environment it represents, and the reviewer who accepted it.
- Refresh evidence after material changes to authentication, banking integrations, endpoint management, or production access tooling.
- Do not publish OTPs, tokens, phone numbers, email addresses, bank details, personal device identifiers, or provider account IDs.

Exceptions

If a requested screenshot cannot be captured safely, CIC must record:

- The reason the screenshot is unavailable.
- The compensating evidence provided.
- The risk owner.
- The expected remediation or next capture date.

Review

This evidence pack must be reviewed at least quarterly and whenever CIC changes MFA, Plaid Link, critical-system access, or endpoint protection tooling.