Credit Bureau Case Study: Phishing-Resistant Authentication Across Five Surfaces

Customer Stories / Last updated 2026-06-11 / https://www.scrambleid.com/learn/case-study-credit-bureau

> **Customer:** One of the three major United States credit reporting agencies. Multi-surface deployment of ScrambleID across voice, web, agent, people, and frontline. One of multiple ScrambleID production deployments; this is the one with results approved for publication.

In one sentence: One of the three major US credit bureaus deployed ScrambleID's phishing-resistant cryptographic authentication across five surfaces (voice, web, agent, people, frontline) on ScrambleID's standard two-week deployment pattern, and approved publication of a 90%-plus reduction in password reset tickets and a 34% improvement in caller verification handle time.

What the customer says

> "We eliminated security questions on day one. Password reset tickets dropped over 90% in sixty days. Employees are actually asking for this. First time I've seen that with a security tool."
>
> *VP of Identity & Access Management at the customer*

That quote captures the practical outcome. Three things in it matter.

First, "security questions on day one" means knowledge-based authentication (KBA) was eliminated, not phased out. KBA is one of the dominant attack surfaces in contact center fraud (see KBA is dead: a contact center playbook for replacing security questions) and removing it cleanly on day one of deployment is a meaningful operational claim.

Second, "90% drop in 60 days" is reset-ticket volume, not authentication volume. That's the metric that flows into operational cost (see the metrics and ROI playbook for how this compounds). At that scale, the operational saving is material.

Third, "employees asking for this" is the cultural signal. Authentication tools with friction get worked around; authentication tools that feel faster get adopted. The reset-ticket reduction is partially mechanical (passwordless eliminates many reset paths) and partially cultural (users self-serve through passkey re-enrollment instead of opening a ticket).

Why this customer is a meaningful reference

The credit bureau operates under unusual scrutiny. As one of the three major US credit reporting agencies, the company sits under FTC, CFPB, and state attorney general oversight. The 2017 data breach (resolved through settlements and remediation costs exceeding $1.4 billion) put the bureau's security posture in the public record in a way that few enterprises ever experience. Every subsequent security investment is visible to regulators, journalists, and the customer base that has reasons to ask hard questions.

For a security buyer evaluating phishing-resistant authentication, that scrutiny is the point. The bureau's authentication architecture has to hold up to:

- **Regulatory audits** (FFIEC IT Examination Handbook, NIST SP 800-63-4, NYDFS Part 500 if any New York-regulated entities are in scope, FTC consent orders post-2017).
- **Public disclosure obligations** (any meaningful security control change becomes part of the next annual report and proxy filings).
- **A workforce and contact-center scale** large enough that day-one rollouts are operationally consequential.
- **Counterparty diligence** from the major banks, fintechs, and government agencies that depend on the bureau's data feeds.

If the architecture works at the credit bureau, it works at other regulated enterprises that have less public exposure but face the same threat model.

The deployment: five surfaces, one rail

The credit bureau deployed ScrambleID across all five surfaces concurrently rather than sequentially. The five surfaces in the deployment:

- **Voice.** Caller verification on inbound contact-center calls. Replaces KBA with cryptographic proof confirmed in the ScrambleID app before the agent picks up. See the Caller Authentication article for the architectural pattern.
- **Web.** Workforce SSO with passkeys and QR-based dynamic identifiers. Federates to the bureau's existing identity provider. See Phishing-Resistant Web Authentication.
- **Agent.** Cryptographic identity for AI agents and service accounts. Replaces long-lived shared secrets with short-lived cryptographic credentials issued per session. See AI Agent Authentication and M2M Authentication Without Secrets.
- **People.** Person-to-person verification for high-risk transactions and helpdesk interactions. Defeats voice-clone and video-deepfake impersonation patterns deterministically. See People Trust Checks and Stopping Helpdesk Impersonation.

- **Frontline.** Shared-device authentication for clean-room and operational environments. No personal phone required. See Desktop Deployment Guide.

The timeline reflects ScrambleID's standard two-week deployment pattern run in parallel, not a sequence of per-surface projects. The architectural enabler is that all five surfaces run on the same cryptographic identity rail (see The Identity Fabric), so a single user enrollment authenticates everywhere. Voice doesn't need its own credential. The AI agent identity doesn't need its own secret-rotation pipeline. The frontline shared-device login doesn't need a separate badge system.

For a deeper look at the overlay model that makes this work, see the Architecture page.

What the published metrics actually mean

Two numbers are public. The 90%-plus reset-ticket reduction appears in the IAM leadership testimonial quoted above; the 34% caller-verification improvement was shared by the customer's IAM leadership for publication by ScrambleID:

Metric	What it means in operational terms
90%+ reduction in password reset tickets	Within sixty days of voice surface rollout. The reduction is not 100% because account recovery, lost devices, and onboarding still generate identity events. The 90% figure is the share of legacy reset-ticket volume that disappears when the password is the credential being eliminated, not just supplemented.
34% faster caller verification	On inbound calls to the contact center. The improvement reflects elimination of the verification step (up to a minute of security questions and re-asks per call), not total call duration. The savings flow through to agent handle time, contact-center capacity, and the per-caller experience.
Two-week deployment pattern	Time from project start to a surface live in production. The credit bureau ran the pattern concurrently across all five surfaces rather than sequentially. The bottleneck in most enterprises is integration with the existing identity provider, contact-center platform (Five9, Genesys, NICE), and helpdesk workflows.

These numbers are what the customer has chosen to share publicly. Internal numbers may be larger or smaller depending on scope; any deeper figures reside under customer-controlled disclosure.

The value of going multi-surface from day one

Most enterprise authentication programs roll out one surface at a time. Web first (because it's the most measurable), then voice, then agents, then people, then frontline. Each surface gets its own vendor evaluation, its own deployment cycle, its own user-enrollment moment. The user ends up enrolled in three or four different authenticators by the end. Helpdesk burden compounds. Cross-surface attack paths (a vector that fails on the web SSO but succeeds via the contact center) stay open the entire time.

The credit bureau did not do that. The five-surface concurrent deployment closes the cross-surface attack paths in one motion. An attacker who tries to breach via voice is hitting the same cryptographic identity that authenticates the user on web. There is no seam. The user enrolls once, and every surface works.

This is the architectural story most enterprises miss when they evaluate passwordless: per-surface point solutions create exactly the seams that adversaries route through. The credit bureau's deployment is the counter-example, executed at scale, in production, under regulatory scrutiny.

What other enterprises can take from this

Three generalizable lessons from what the customer has disclosed publicly.

1. Pick the surface with the most operational pain to demonstrate value. The credit bureau led with voice. KBA in a contact center is high-volume, high-friction, high-fraud-cost; eliminating it produces a measurable result in weeks rather than quarters. Wins on that surface build the political capital to take the rest.

2. Run the surfaces concurrently, not sequentially. The two-week pattern is the architectural payoff. Each surface does not need to be its own twelve-month project. The federated identity model means the integration work compounds rather than replicates.

3. Plan for the cultural moment, not just the security control. "Employees asking for this" is the line that reads like marketing but matters operationally. Adoption is the leading indicator that the deployment will hold; resistance is the leading indicator that you have a process problem disguised as a tech problem.

For the implementation playbook, see the metrics and ROI playbook and the omnichannel authentication guide.

Looking ahead

The bureau's authentication program continues to evolve as threats do. AI-driven social engineering against contact centers, agent identity for AI workloads, and the publication of NIST SP 800-63-4 (finalized July 2025) are all active areas where the deployment will continue to adapt. ScrambleID's role is to provide the cryptographic identity rail that scales with those changes; the architectural choices the bureau made in the original deployment compound across each new control objective rather than requiring re-architecture.

For other regulated enterprises considering a similar deployment, the most useful artifact is the evaluation checklist and RFP guide, which translates the architectural pattern into procurement-stage questions you can take into your own vendor evaluation.

FAQ

What surfaces did the customer deploy ScrambleID across?

The credit bureau deployed ScrambleID across all five surfaces: voice (caller verification in the contact center), web (workforce SSO), agent (AI and service-account identity), people (in-person and high-risk transaction verification), and frontline (shared-device and clean-room authentication). The same cryptographic identity authenticates across every surface.

How long did the deployment take?

The deployment followed ScrambleID's standard two-week pattern, run concurrently across all five surfaces. A single enrollment authenticates everywhere, so each surface lights up on the same rail instead of becoming its own project.

What measurable outcomes has the customer disclosed publicly?

The customer has approved publication of two measurable outcomes from the ScrambleID deployment: more than 90% reduction in password reset tickets (within sixty days of voice surface rollout) and 34% faster caller verification on inbound calls to the contact center. The deployment itself followed ScrambleID's standard two-week pattern run concurrently across all five surfaces. The reset-ticket figure is quoted in the IAM leadership testimonial above; the caller-verification figure was shared by the customer's IAM leadership for publication by ScrambleID.

Why is this credit bureau a meaningful reference for enterprise security buyers?

Three reasons. First, scale: the bureau operates one of the largest data-sensitive workforces and contact centers in financial services, so any authentication architecture that holds up there demonstrates enterprise readiness. Second, regulatory exposure: as one of the three major US credit bureaus, it operates under FTC, CFPB, and state attorney general oversight, plus public scrutiny from the 2017 breach aftermath. Third, integration depth: a five-surface deployment exercises the full omnichannel architecture, not just the web login surface.

Can other enterprises replicate this deployment pattern?

Yes. The deployment pattern (federate to the existing IdP, layer ScrambleID across all five surfaces, enroll users once for the whole rail) is documented in the Learn hub and is the same pattern other ScrambleID customers run. This customer's timeline and metrics are not guaranteed for every deployment, but the architectural model is general.

Key Takeaway

One of the three major United States credit reporting agencies deployed ScrambleID across all five surfaces (voice, web, agent, people, frontline) on ScrambleID's standard two-week deployment pattern, run concurrently, and approved publication of two operational outcomes: more than 90% reduction in password reset tickets within sixty days of voice surface rollout, and 34% faster caller verification in the contact center. The case is meaningful because the credit bureau operates under exceptional regulatory and public scrutiny (FTC, CFPB, NYDFS, post-2017-breach disclosure obligations) and because the five-surface concurrent deployment closes cross-surface attack paths that per-surface point solutions leave open. The architectural enabler is a single cryptographic identity rail that authenticates the user on web, voice, AI agent, in-person, and shared-device contexts; the user enrolls once and authenticates everywhere. The deployment pattern is documented and replicable for other regulated enterprises.

References (public)

- Customer testimonial: shared by the customer's IAM leadership for publication by ScrambleID (quoted in full above)
- ScrambleID llms.txt customer manifest: the credit bureau deployment listed among ScrambleID's production deployments (voice, web, agent, people, frontline)
- NIST SP 800-63-4 Digital Identity Guidelines: the standard ScrambleID deployments are designed to support
- CISA Implementing Phishing-Resistant MFA: federal guidance that the architecture meets

Related reading

- Omnichannel Authentication: Proof, Not Probability: the architectural pattern the credit bureau deployed
- Metrics and ROI Playbook: how to model the operational savings the published metrics imply
- Caller Authentication: Replace KBA and Stop Vishing: the voice-surface canonical
- ScrambleID Architecture: One Identity Fabric: the rail that lets a single enrollment span five surfaces
- Evaluation Checklist and RFP Guide: translating this pattern into procurement-stage questions