BANKNOTE SECURITY · A MASTER CLASS

Banknote security has three layers. You only see one.

Banknote security is the most successful authentication system ever built. Counterfeit rates run in single digits per million notes. Most of the reasons are invisible by design, and they map onto every other industry now trying to authenticate physical products.

BY JOHN WOLFE · CEO, NOVAVERA

THE SCALE

Banknote counterfeiting is rare. Almost everything else isn't.

BANK OF CANADA · 2024

9

counterfeit notes per million in circulation

GLOBAL IMPORTS · 2021

2.3%

were counterfeit goods (roughly 23,000 ppm by value)

G7 and Eurozone economies hold counterfeit banknote rates under 30 parts per million. Counterfeit goods run thousands of times higher in consumer markets. The reasons aren't accidental. They're designed.

SOURCES: BANK OF CANADA 2024 ANNUAL REPORT · OECD/EUIPO MAPPING GLOBAL TRADE IN FAKES 2025

THE ARCHITECTURE

Banknote security is built in three layers.

01

Public-facing features. Watermarks, holograms, color-shifting ink, raised intaglio printing.

FOR: CITIZENS · VERIFICATION: VISIBLE · TIME: SECONDS

02

Machine-readable features. Infrared inks, magnetic strips, ultraviolet fluorescence, embedded threads.

FOR: CASH HANDLERS · VERIFICATION: COVERT · TIME: MILLISECONDS

03

Forensic features. Materials and signatures only the issuing central bank can detect or describe.

FOR: CENTRAL BANKS · VERIFICATION: UNDISCLOSED · TIME: LAB

LEVEL 01 · PUBLIC-FACING

What you see on a banknote is for you.

Visible features are designed for citizen-level verification. The watermark you tilt to the light, the foil patch that changes color, the raised feel of intaglio under your thumb. These exist so that any person can confirm a note is real in seconds, without equipment.

Watermarks
Embedded in the substrate during papermaking

Intaglio printing
Raised lines you can feel

Holograms / OVDs
Optically variable foil patches

Color-shifting ink
Changes hue when tilted

Level 1 features are the part of banknote security **built for the user, not against the counterfeiter.**

LEVEL 02 · MACHINE-READABLE

Cash handlers see what citizens don't.

A second tier of features is invisible to the naked eye but legible to ATMs, sorters, and tellers' verification machines. Infrared and ultraviolet response, magnetic ink, and embedded thread codes let machines authenticate a note in milliseconds, often without the operator even seeing it happen.

Infrared (IR) inks
Visible only under IR illumination

Ultraviolet (UV) fluorescence
Activates under UV light

Magnetic security threads
Encoded magnetic signatures

Embedded fluorophores
Spectral signatures inside paper

Level 2 features are **covert by design.** Most are never disclosed publicly. That's part of how they work.

LEVEL 03 · FORENSIC

The deepest layer is the one nobody talks about.

Every G7 banknote is understood to carry forensic features that only the issuing central bank can verify. Their existence is acknowledged. Their identity is not. These are the features that resolve a counterfeit dispute when every other layer is in question. They are deliberately kept secret because secrecy is part of their security.

Embedded materials
Specific chemical or optical signatures

Lab-only signatures
Detected by the central bank, nobody else

Reserved features
Some defenses are held in reserve

Disclosed: zero
By policy, not omission

If counterfeiters don't know a feature exists, they cannot copy it. **Secrecy is not weakness here. It's the design.**

THE PATTERN

Visible features satisfy the user. Machine-readable features run the system. Forensic features hold the line.

The features that secure money are the ones you don't see.

WHY THIS MATTERS ELSEWHERE

What banknote security can teach the rest of the world.

01 **Layer the defense.** A single feature can fail. A stack of features fails together only when each one fails, and they don't fail at the same time.

02 **Make the real security covert.** The features citizens or buyers can see should not be the features that protect the product. They should reassure; the real defense should be invisible.

03 **Build authentication into the material.** Banknote substrates carry security features inside them, not stuck to them. Anything applied can be lifted. Anything embedded can't.

04 **Iterate continuously.** Central banks redesign banknotes every 10 to 20 years and continually update production techniques between cycles. Static security is degrading security.

ENGINEERING REFERENCE

From central banks to commercial brands.

Covert taggants embedded directly into the banknote substrate during manufacturing carry luminescent or spectroscopic signatures that only authorized readers can detect. Public vendor disclosures place this category of authentication in central bank programs for over fifteen years. The same engineering, embedded, machine-readable, layered, and quantitatively detected, is now being applied to luxury goods, pharmaceuticals, industrial materials, and high-value parts.

THREE THINGS TO TAKE FROM THIS

What this brief tried to make visible.

01 Banknote security works because it's layered, mostly invisible, and continually iterated. Counterfeit rates measured in single-digit parts per million are the result.

02 The visible security features serve the user, not the security model. The real defense is at Levels 2 and 3: covert, machine-readable, forensic.

03 The principles are not exclusive to currency. Any product worth authenticating can borrow the same architecture: embedded, layered, covert by default.

John Wolfe is CEO of NovaVera, which builds authentication infrastructure for high-stakes products: currency, pharmaceuticals, luxury goods, and industrial materials. Field Notes is a series for practitioners. Follow NovaVera for the next briefing.