



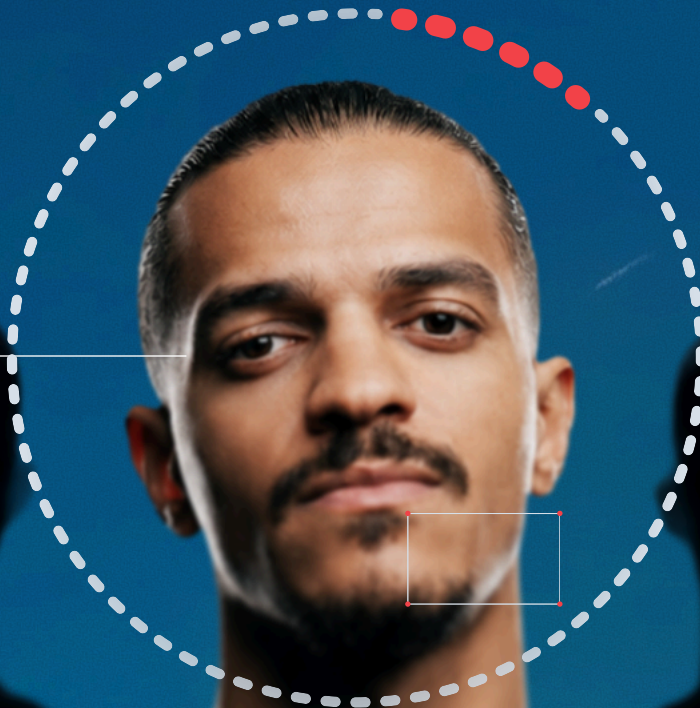
# The North America Guide to Docless Identity Verification

How to reduce document-upload friction without weakening CIP or FINTRAC compliance.

Liveness



Passed



KJM Age  
Verification



PCI DSS



iBeta Level 3



ISO/IEC  
27001:2022



CE+



QG GDPR



SOC2



GDPR



CCPA



# Table of Contents

|    |                                                                                             |    |
|----|---------------------------------------------------------------------------------------------|----|
| —  | <b>Introduction</b>                                                                         | 03 |
|    | The first attempt to verify a customer is the one that decides the economics.               |    |
| 01 | <b>North America's onboarding problem</b>                                                   | 04 |
|    | Record fraud losses, upload abandonment, and synthetic identity.                            |    |
| 02 | <b>How Docless Identity Verification works</b>                                              | 06 |
|    | Passive, Active, and Biometrically Enriched.                                                |    |
| 03 | <b>Docless verification is written into the law</b>                                         | 08 |
|    | The US CIP rule and Canada's FINTRAC methods.                                               |    |
| 04 | <b>The verification rails</b>                                                               | 12 |
|    | Credit bureaus, government match services, and the mDL shift.                               |    |
| 05 | <b>The risk routing model</b>                                                               | 16 |
|    | Passive first, biometric bind for synthetic risk, documents as fallback.                    |    |
| 06 | <b>Shufti's North America coverage</b>                                                      | 18 |
|    | eIDV, document verification, and live mDLs through one integration.                         |    |
| 07 | <b>Alongside eIDV</b>                                                                       | 20 |
|    | US AML obligations, Canada's Bill C-12 penalties, and biometric privacy laws.               |    |
| 08 | <b>Getting started</b>                                                                      | 22 |
|    | Configuration add-on, scoping call, or due-diligence pack, plus frequently asked questions. |    |
| —  | <b>References</b>                                                                           | 25 |
|    | All thirteen sources, with URLs intact.                                                     |    |



# The regulation describes the database check. The industry habit is the document upload.

The first attempt to verify a customer is the one that decides the economics. When an identity confirms on the first pass, the customer moves straight into the product and the compliance record is complete from the outset. When it fails, a share of genuine applicants walk away, a manual review queue forms, and the same regulatory duty gets discharged twice at higher cost.

North America adds a twist that most onboarding teams have never examined. There is no national ID in the United States or Canada, and because of that, the identity rules in both countries were drafted around something else entirely. They describe matching a person's details against consumer reporting agencies, government records, and other authoritative sources. This guide is about closing the gap between what the regulation describes and what the industry does by habit. The stakes are higher than they were five years ago, when a photographed document was still hard to fake and synthetic identity was a niche typology rather than the signature fraud of the region.

## 48.3%

of US banked households used mobile banking as their primary way to access an account in 2023, roughly nine times the share of a decade earlier.

SOURCE: FDIC, 2023 NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS

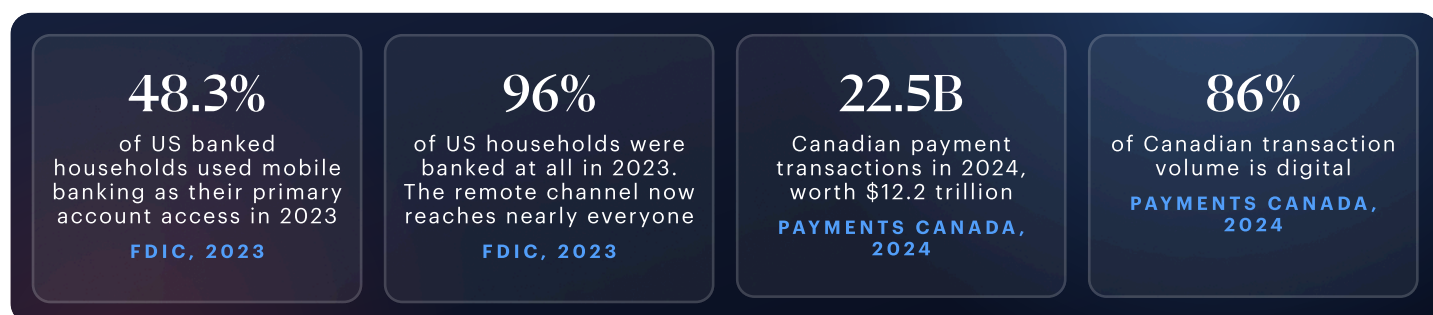
One more thing has changed since those rules were written. The United States never built a national eID, but it is getting the next closest thing. More than 20 states plus Puerto Rico now issue mobile driver's licences (mDLs), cryptographically signed credentials that live in a phone wallet, and NIST is drafting the playbook for banks to accept them in customer identification. For the first time, the US has a sovereign digital credential to verify against, and this guide covers where it fits.

What follows shows how businesses can use Docless Identity Verification to raise first-pass success, counter synthetic identity fraud, and meet the letter of the CIP and FINTRAC frameworks. A practitioner guide for compliance, product, and onboarding teams.

# Document-first onboarding can lose customers and miss synthetic ID fraud.

Digital account opening is no longer a minority path in either country. Every new account behind the volume below needs an identity check, and most of those checks happen with no branch, no counter, and no human on the other side.

## THE VOLUME



Sources: FDIC 2023 National Survey of Unbanked and Underbanked Households; Payments Canada, Canadian Payment Methods and Trends 2025.

### PROBLEM 01

#### The step where genuine users quit

The capture step is the highest-friction moment in remote onboarding. Applicants asked to find a physical document, photograph it in good light, and retry after a blurred frame abandon here more than at any other step, a pattern verification teams across the region see consistently in their own funnels. Users lost here are rarely recovered.

### PROBLEM 02

#### The step where fraud now walks in

Generative AI has made convincing fake identity documents cheap to produce at scale. The photographed document, the exact artefact the default flow is built around, is the artefact that generative tooling now targets.



## 01 — NORTH AMERICA'S ONBOARDING PROBLEM

The fraud pressure has scaled with the channel. Identity fraud was the most common fraud type in the Canadian Anti-Fraud Centre's 2024 reporting, and every headline number below set a record in the 2025 cycle.

### THE FRAUD



All figures neutral-sourced: FTC, FBI IC3, Competition Bureau Canada, FinCEN via GAO.

#### NOV 2024 FinCEN's deepfake alert

FinCEN warned financial institutions that criminals use deepfake media, including fabricated identity documents, specifically to defeat identity verification controls, and that suspicious-activity filings tied to this behaviour had risen. **FinCEN Alert FIN-2024-Alert004.**

There is a third problem underneath both, and it is distinctly North American. Because the US has no national ID and Social Security numbers are not verified in real time at issuance of most accounts, criminals fabricate people, combining a real SSN with an invented name and date of birth and letting the synthetic profile mature. A document photo does nothing against this, because the synthetic applicant is presenting a person who does not exist rather than impersonating someone real.

**The core insight.** A flow that runs every applicant through the same document check concentrates friction on the genuine majority while leaving the region's signature fraud unaddressed. The alternative is to verify low-risk users against the authoritative data both regulators already point to, add a biometric bind where synthetic identity is the threat, and reserve the document flow for the cases that need it.

# Docless verification works in three layers of assurance.

Shufti's eIDV solution offers three verification methods, each built for a different assurance level and user journey. In North America the three do not carry equal weight, and understanding why is most of the deployment decision.

## METHOD 01 · THE NORTH AMERICAN HERO

NO USER ACTION

### Passive Verification

The user provides their name, date of birth, address, and a national identifier such as an SSN, and the match runs in the background against trusted sources, credit bureaus, government records, and other authoritative databases. From the user's side there is nothing beyond the form they were already filling in. This is the route both the US CIP rule and Canada's FINTRAC credit-file method describe.

SHUFTI PASSIVE CHECKS RUN AGAINST 230+ AUTHORITATIVE DATABASES WORLDWIDE

## METHOD 02

### Active Verification

The user proves who they are through a credential they already hold, a bank or government eID login, or a government-issued digital credential presented from a wallet, and the issuer confirms the identity in real time. The mDL changes what Active means in America, returning issuer-verified attributes with no document image and no OCR.

CANADA: INTERAC + PROVINCIAL IDS

US: MDLS LIVE TODAY

## METHOD 03

### Biometrically Enriched

A live selfie is matched against the photo held by the authoritative source, layered on top of the Passive or Active data match. Configurable as 1+1 (single source) or 2+2 (dual-source cross-reference), the second designed to flag identities whose attributes do not reconcile across independent sources.

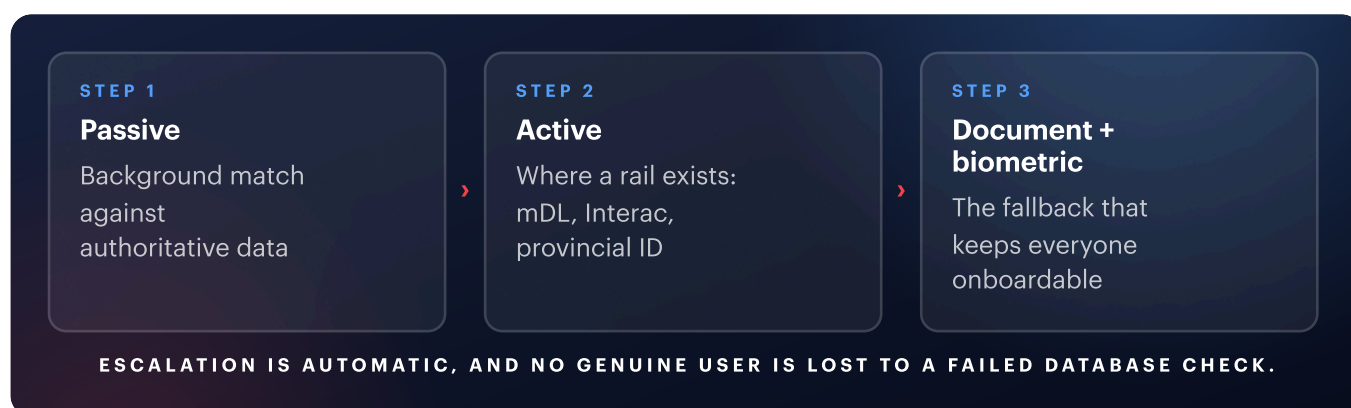
COUNTERS SYNTHETIC IDENTITY

MDL PORTRAIT CAN BE THE MATCH SOURCE

Three methods, one flow. Passive carries the low-risk majority. The fallback strip continues overleaf.

# Failed data checks should step up, not stop onboarding.

Not every check returns a confident match. Shufti's Journey Builder escalates automatically, from Passive to Active where a rail exists, or to document verification with biometric matching, so no genuine user is lost to a failed database check. The escalation logic sits in configuration, not in code.



## SHUFTI COVERAGE — PRODUCT CLAIMS

Authoritative databases for Passive checks

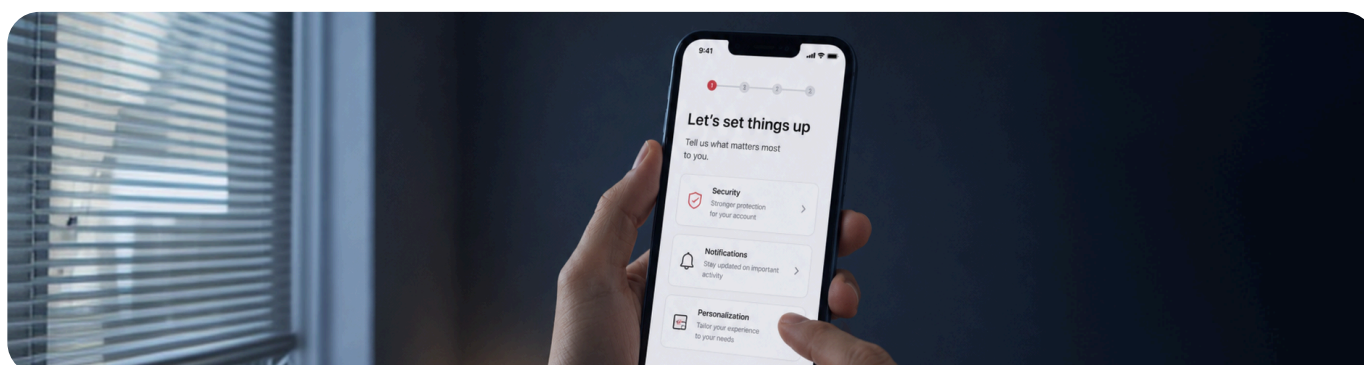
230+

National eID schemes for Active verification

40+

US mobile driver's licences

Live today,  
additional states on client demand



## US and Canadian rules already permit docless verification.

This is the section that separates North America from every other region. Elsewhere, the docless case usually rests on a regulator having permitted electronic verification. Here, the docless route is named in the regulation text itself, under the regulator's word for it, *non-documentary*, and it has been there for over two decades.

### UNITED STATES — NON-DOCUMENTARY VERIFICATION UNDER THE CIP RULE, 31 CFR 1020.220

The load-bearing authority is the Customer Identification Program rule. Under Section 326 of the USA PATRIOT Act (codified at 31 U.S.C. 5318(l)), FinCEN's CIP rule for banks at 31 CFR 1020.220 permits non-documentary identity verification and lists the methods in the regulation's own words, set out in full on the facing page. The same non-documentary provision appears in the parallel CIP rules for broker-dealers (31 CFR 1023.220), mutual funds (31 CFR 1024.220), and futures commission merchants and introducing brokers (31 CFR 1026.220). The rule also names the exact situation remote onboarding creates, the customer who "opens the account without appearing in person."

Three supporting instruments round out the picture.

#### FFIEC BSA/AML EXAMINATION MANUAL

Instructs examiners to review accounts opened through both documentary and non-documentary methods, which makes docless onboarding an examined, accepted practice rather than a grey area.

#### NIST SP 800-63-4 DIGITAL IDENTITY GUIDELINES

Sets the Identity Assurance Level framework (IAL1 through IAL3) used to calibrate remote identity proofing. Revision 4, including SP 800-63A-4 on identity proofing, was published final on 31 July 2025.

#### NIST SP 1800-42A (DRAFT, MAR 2026)

In March 2026, NIST's National Cybersecurity Center of Excellence released the initial public draft of a reference architecture for financial institutions accepting mobile driver's licences in customer identification, built with 29 industry and government collaborators. The comment period closed in May 2026. The CIP rule was always technology-neutral. This is the document that turns mDL acceptance from a legal possibility into an examinable practice.



# THE REGULATION

“

These methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a **consumer reporting agency, public database, or other source**, checking references with other financial institutions; and obtaining a financial statement.”

---

**31 CFR 1020.220(a)(2)(ii)(B)(1)**

THE US CUSTOMER IDENTIFICATION PROGRAM RULE



## 03 — WRITTEN INTO THE LAW

### CANADA — CREDIT-FILE AND DUAL-PROCESS METHODS UNDER THE PCMLTFA

The governing statute is the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA, S.C. 2000, c. 17), with verification methods prescribed in its regulations (PCMLTFR, SOR/2002-184).

FINTRAC's guidance on methods to verify the identity of persons and entities sets out the permitted routes, and two of them are docless by design.

| DOCLESS BY DESIGN                                                                                                                                                                                                                                                                                                                                           | DOCLESS BY DESIGN                                                                                                                                                                                                                                                                                    | TECHNOLOGY-ASSISTED                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CREDIT-FILE METHOD</b><br>A single Canadian credit file can verify identity on its own, provided it is current, comes from a Canadian credit bureau, has existed for at least three years, draws on more than one source, and matches name, address, and date of birth. The search must run at the time of verification. A stored copy does not qualify. | <b>DUAL-PROCESS METHOD</b><br>Identity verified using information from two different reliable sources, drawn from combinations of name + address, name + date of birth, or name + a confirmed financial account. A Canadian credit file at least six months old can serve as one of the two sources. | <b>PHOTO-ID METHOD</b><br>For a person not physically present, the process must authenticate the document using reliable technology, while ensuring it is valid, current, and matches the person's name and photo. A live video chat can confirm the match but cannot replace document authentication. |

Source: FINTRAC methods guidance under the PCMLTFA.

The credit-file backbone is named in the guidance itself, Equifax Canada and TransUnion Canada. Document verification in Canada is therefore already a technology-assisted process by regulatory requirement, not by vendor preference.

FINTRAC also permits an **affiliate or member method** and a **reliance method**, allowing reuse of a prior verification under defined conditions. The PCMLTFA and its regulations were amended across 2025, and compliance teams should confirm the current consolidated text before relying on any single provision.

**“It is not enough to only view a person and their government-issued photo identification document through a video conference or another type of virtual application.”**

VIDEO IS NOT RULED OUT. FINTRAC ACCEPTS A LIVE VIDEO CHAT TO COMPARE THE PERSON AGAINST THE PHOTO ON THE DOCUMENT. WHAT IT REJECTS IS VIDEO STANDING IN PLACE OF AUTHENTICATING THE DOCUMENT IN THE FIRST PLACE.

### **What the United States' and Canada's eIDV frameworks have in common**

Neither country treats docless verification as an exception to be justified. Both describe it as a standard route, specify what sources qualify, and expect the same record-keeping either way.

The question a North American compliance team faces is not whether the regulator permits a database check. It is whether their current onboarding flow reflects what the regulator already wrote.

#### **Does your onboarding flow reflect what the regulator wrote?**

Shufti's North America team can walk your current flow through the CIP and FINTRAC methods and show where a docless route already fits.

**Book a demo**

# US identity checks are credit-led, but mobile IDs are opening a new path.

A regulation that permits database checks is only useful if the databases exist and can be queried. In both countries they do, and the picture per country is worth setting out precisely, because the rails differ in kind from the national-ID systems that carry eIDV elsewhere.

## Credit bureaus and credit-header data **THE WORKHORSE**

The three nationwide consumer reporting agencies, Experian, Equifax, and TransUnion, function as the country's de facto identity rails. Credit-header data, the identifying top section of a credit file covering name, current and prior addresses, SSN, and date of birth, is the workhorse of US eIDV matching. A December 2024 CFPB proposal would have brought header data inside the FCRA's consumer-report regime, but the Bureau withdrew it in May 2025, and header-based verification continues to operate as before.

## SSA eCBSV **GOVERNMENT MATCH**

The Social Security Administration's electronic Consent Based SSN Verification service confirms whether an SSN, name, and date of birth combination matches SSA records, returning a yes or no with the number holder's consent. It launched in June 2020 expressly to reduce synthetic identity fraud.

## AAMVA DLDV **GOVERNMENT MATCH**

The Driver's License Data Verification service checks driver's licence and state ID data against the issuing motor vehicle agency's records, returning per-element match flags without releasing the underlying data.

## Mobile driver's licences **NOW LIVE**

States issue cryptographically signed mDLs built to ISO/IEC 18013-5, coordinated through AAMVA, whose Digital Trust Service anchors issuer authentication. More than 20 states plus Puerto Rico issue them as of early 2026 (AAMVA jurisdiction data), a count that still moves quarterly. The spotlight overleaf sets out why this is the region's most consequential eIDV development.



# Mobile driver's licences are America's eID moment.

Until now, the Active method has mapped to Canada and Europe rather than to the US, because there was no US credential to present. The mobile driver's licence changes that. An mDL is issued by a state motor vehicle agency, signed cryptographically by the issuer, and held in a phone wallet. ISO/IEC 18013-7 extends presentation over the internet, which is what makes an mDL usable inside a remote onboarding flow.

## REMOTE PRESENTATION, STEP BY STEP

- 1 The wallet holds the mDL**  
A state-issued, cryptographically signed credential on the applicant's phone.
- 2 ISO/IEC 18013-7 presentation**  
The holder approves exactly what is shared. **SELECTIVE DISCLOSURE** Shares only what is requested: age, address.
- 3 Issuer signature validated**  
The credential is checked against the state issuer's cryptographic signature.
- 4 Attributes + compliance record delivered**  
Verified attributes arrive with the audit trail the business answers examiners with.

## THE MILESTONES

- OCT 2024**  
ISO/IEC 18013-7 published, remote presentation standardised
- TODAY**  
TSA accepts mDLs at 250+ airport checkpoints
- EARLY 2026**  
More than 20 states plus Puerto Rico issuing (AAMVA jurisdiction data)
- MAR 2026**  
NIST SP 1800-42A draft for mDL-based CIP
- LIVE WITH SHUFTI**  
Today, remaining states on client demand

What the wallets do not provide is the layer businesses answer audits with. Someone still has to validate the issuer signature, cover the wallet and state fragmentation, route the users who do not hold an mDL, and keep the compliance record. That orchestration is the role Shufti's eIDV hub already plays for 40+ national eID schemes worldwide.

Coverage arrives state by state and wallet by wallet, which is exactly why it needs an orchestration layer.

# Canada's identity checks are credit-led, bank-linked, and province-by-province.

## Credit bureaus **NAMED IN THE GUIDANCE**

Equifax Canada and TransUnion Canada are the backbone of the FINTRAC credit-file method, named in the guidance itself.

## Interac verification services **BANK-LOGIN RAIL**

Bank-login verification lets a user confirm identity through their existing financial institution credentials, and Interac's document verification service adds facial biometric liveness. These are enterprise services and remain live. The earlier consumer-facing verification app was retired, so flows should reference the current service names.

## Provincial digital IDs **STATE OF PLAY**

The BC Services Card and [Alberta.ca](https://alberta.ca) Account are live digital identity solutions. Quebec gained legal authority for its digital identity program on 28 October 2025 through Bill 82 (S.Q. 2025, c. 26). Ontario has no live digital ID; its program is shelved and should not be considered an available option.

## DIACC Pan-Canadian Trust Framework **FRAMEWORK, NOT A RAIL**

An industry certification framework for identity interoperability. It is a framework, not a live credential, and belongs in vendor due diligence conversations rather than onboarding flows.



# The US and Canada side by side: rules, rails, and fraud pressure

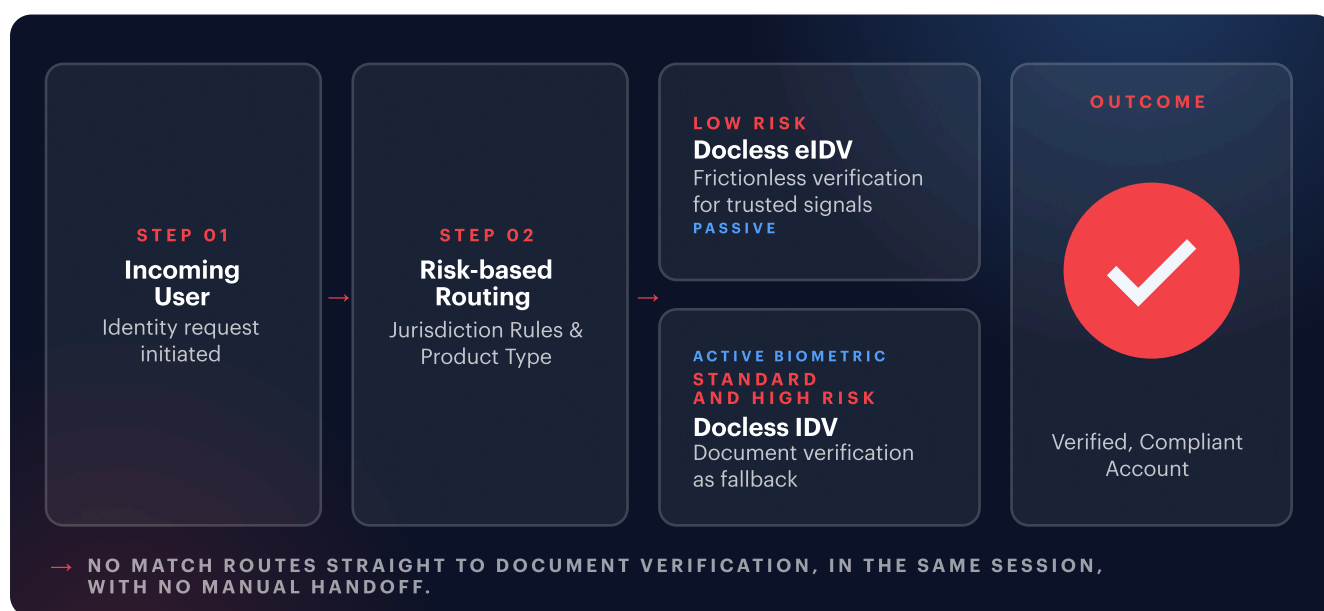
|                                                   | UNITED STATES                                                                           | CANADA                                                           |
|---------------------------------------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------|
| <b>National ID</b>                                | None                                                                                    | None                                                             |
| <b>Regulatory basis for docless verification</b>  | CIP rule, 31 CFR 1020.220 and parallels, under USA PATRIOT Act s.326                    | PCMLTFA and PCMLTFR, with FINTRAC methods guidance               |
| <b>Named non-documentary method</b>               | Match against a consumer reporting agency, public database, or other source             | Credit-file method and dual-process method                       |
| <b>Credit-bureau rail</b>                         | Experian, Equifax, TransUnion (credit-header data)                                      | Equifax Canada, TransUnion Canada                                |
| <b>Government match services</b>                  | SSA eCBSV (SSN, name, DOB), AAMVA DLDV (driver's licence)                               | Provincial registries, bank-login verification via Interac       |
| <b>Sovereign credential or eID login (Active)</b> | <b>mDLs, live in early states and expanding</b> , with remote presentation standardised | Interac bank login, provincial digital IDs (BC, Alberta, Quebec) |
| <b>Assurance framework</b>                        | NIST SP 800-63-4, IAL1 to IAL3 (final July 2025)                                        | FINTRAC method framework                                         |
| <b>Signature fraud pressure</b>                   | Synthetic identity (real SSN, fabricated person)                                        | Identity fraud, the most-reported fraud type (CAFC 2024)         |





# Start docless, then step up only when risk demands it.

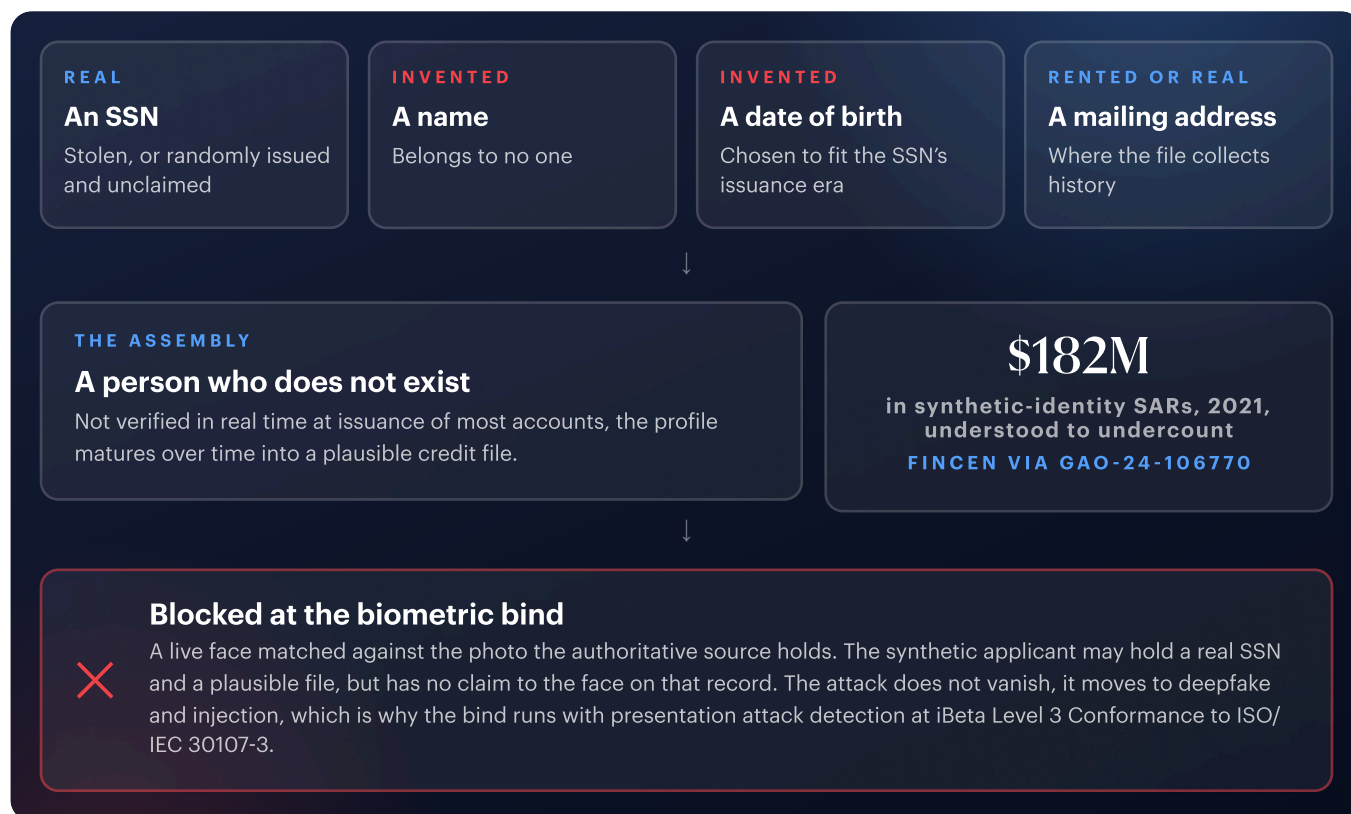
The practical question for a North American onboarding team is how to route each applicant, using risk level, data availability, and the fraud typology this region actually produces.



The fallback step is what makes the model safe to deploy. Database coverage is broad in both countries, but no source covers everyone. Recent immigrants, young applicants with no credit history, and anyone with a thin or absent bureau file will not always clear a Passive check. An automatic route to the document flow keeps them onboardable while everyone else skips the step entirely.



# Synthetic identity blends real data with a fake person.



Stolen data carries the synthetic applicant as far as the biometric step. Getting past that step costs far more, and leaves far more evidence.

**Why the synthetic emphasis matters.** A routing model imported from Europe or APAC treats biometric enrichment as a premium tier for high-value accounts. In North America it belongs in the mainstream risk logic, because the signature fraud is a fabricated person with real-looking data. A live face bound to the authoritative record is the one check the synthetic applicant cannot rehearse.

# One Shufti integration runs the full North American flow.

Businesses onboarding across the US and Canada typically assemble this from parts, one vendor for bureau-based checks, another for document capture, a third for watchlist screening, and internal engineering to hold the seams together. Shufti runs the full routing model through one API.

|         |                        |                                                      |
|---------|------------------------|------------------------------------------------------|
| ONE API | Passive eIDV           | 230+ AUTHORITATIVE DATABASES                         |
|         | Active eIDV            | 40+ NATIONAL eID SCHEMES, INCL. US mDLs              |
|         | Biometrically Enriched | iBETA PAD LEVEL 2                                    |
|         | Document verification  | 10,000+ DOCUMENT TYPES, 240+ COUNTRIES & TERRITORIES |
|         | AML screening          | IN THE SAME FLOW                                     |

Coverage figures are Shufti product claims.

Active verification connects through the same hub that runs BankID, Singpass, and the European schemes, and in North America that now includes the US mDL rail alongside Interac bank login and the provincial digital IDs in Canada. Shufti verifies California and Louisiana mDLs today, returning issuer-signed identity attributes with age and address confirmation in the same journey as every other method. The remaining 19 issuing states on the early-2026 AAMVA count activate on client demand, through configuration rather than new integration work, and the same applies to new wallets as they launch.

Biometrically Enriched verification binds a live selfie to the source record with liveness detection certified to iBeta PAD Level 2. Where the record is an mDL, the match runs against the licence portrait the issuer returns, which answers the case where the phone in the flow is not held by the person the licence belongs to.

99.8%

VERIFICATION ACCURACY

&lt;3 sec

PROCESSING TIME

1,000+

ENTERPRISE CLIENTS

Delivery figures are Shufti's own product claims.

# When docless cannot clear, documents keep users moving.

Shufti's Identity Document Verification supports 10,000+ actively processed document types from 240+ countries and territories, combining OCR, NFC chip reading where the document supports it, and biometric face matching.

## WHY IT MATTERS HERE

North America is a region defined by cross-border movement, a US fintech onboarding a new arrival with a foreign passport, or a Canadian platform verifying a customer whose credit file is six months too young for the credit-file method. In both cases the document route holds the applicant, and the docless route takes over the moment the data exists.

Routing logic lives in Journey Builder configuration, not code, so compliance teams can adjust risk tiers, add a biometric step for a product line, or tighten fallback conditions without an engineering release.

## See the routing model on your own use case

One session maps your products, risk tiers, and markets to the configuration described above, across both countries.

[Book a Demo](#)

## Verification must satisfy AML and privacy at the same time.

Identity verification is the first gate, not the whole obligation. Three adjacent regimes shape how a docless programme should be built in North America.

### US AML OBLIGATIONS

CIP sits inside a wider BSA/AML programme. The CDD rule (31 CFR 1010.230) adds beneficial-ownership requirements for legal-entity customers, and verified identities must be screened against sanctions and watchlists, with suspicious activity reported.

Money services businesses, including most crypto platforms, carry recordkeeping and Travel Rule duties, triggered at the \$3,000 threshold. A 2020 proposal to lower that to \$250 for international transfers has never been finalised, so \$3,000 remains the operative figure.

Shufti runs AML screening in the same flow as verification, so a user verified through either route is screened without a second integration.

### CANADIAN AML OBLIGATIONS

The PCMLTFA regime is becoming stricter. Bill C-12, receiving royal assent on 26 March 2026 as S.C. 2026, c. 4, introduced amendments including a major increase in administrative monetary penalties.

For very serious violations by entities, the maximum penalty rises from \$500,000 to \$20 million, with a cumulative cap of the greater of \$20 million or 3% of global gross revenue at group level. The act also introduces mandatory FINTRAC enrollment across reporting sectors with a public registry, though this provision is not yet in force and should be treated as a future requirement.

The consequences of using an identity-verification method that fails an audit have never been higher in Canada.

# 40×

THE INCREASE ON THE PREVIOUS  
\$500,000 CEILING, UNDER BILL C-12 (2026)

The third regime, biometric privacy, is the overlay teams underestimate, and it operates separately from AML law in both countries. The next page maps it.



# Biometrics add assurance, but privacy must be designed in.

## ILLINOIS

### BIPA (740 ILCS 14, amended 2024)

Requires informed written consent before collecting biometric identifiers, and carries a private right of action.

## TEXAS

### CUBI

Imposes its own notice and consent duties on the capture of biometric identifiers.

## WASHINGTON

### Biometric statute

Notice and consent duties for enrolling biometric identifiers for a commercial purpose.

## QUEBEC

### Law 25 + biometric-database disclosure

Express-consent requirements for biometric matching, plus disclosure to the province's privacy regulator before a biometric database is put into service.

Face verification triggers privacy law that operates separately from AML law, so consent screens and retention limits belong in the flow design.

Federally in Canada, PIPEDA governs, with provincial private-sector laws in Alberta, BC, and Quebec layered on top. None of this argues against biometric verification. It argues for deploying it with consent screens, retention limits, and disclosure practices designed in from the start, and for choosing a verification partner whose flows already accommodate them.

The mDL works in the same direction. Selective disclosure lets a flow request a single attribute, an age threshold or an address, without exposing the rest of the licence, which is the data-minimisation posture privacy regulators keep asking for.

**The practical implication.** A North American verification programme has to satisfy an AML examiner and a privacy regulator at the same time, in two countries. The difference between a programme that can evidence compliance end to end and one that reconstructs it across vendors at audit time is whether verification, biometric consent capture, and AML screening run in one configurable flow.

# Start from your current verification setup.

Docless Identity Verification deploys alongside document verification through one Shufti integration, with no additional API work. The routing sits in configuration. Where a team starts depends on where they stand today.

## Already using Shufti for document verification

Docless verification is a configuration addition to your existing integration. Define which risk tiers route to Passive checks, where the biometric bind applies, and when document verification triggers as step-up, all through Journey Builder, without engineering work.

## Evaluating verification for the first time

Start with a scoping conversation specific to your markets. US and Canadian flows draw on different rails and different regulatory methods, and the right configuration depends on your product type, risk profile, and user base. A scoping call with Shufti's North America team establishes which routes apply before any integration work begins.

## Compliance teams conducting vendor due diligence

Shufti's documentation for North America includes regulatory mapping for the CIP and FINTRAC frameworks, source-type confirmation for eIDV coverage, and biometric-consent flow documentation for the privacy regimes in Section 07. Available on request as part of a vendor assessment.

### THE CASE FOR THE COMBINED APPROACH

Docless verification removes the upload step for the low-risk majority and raises first-pass success. The biometric bind answers synthetic identity. Document verification holds the fallback and the high-risk tiers, with the audit trail regulators expect. One integration runs all of it, in both countries, with AML screening alongside.

[Book a Demo](#)

# Questions buyers ask before switching to docless.

## Q1 Is docless identity verification legal in the United States?

Yes. The CIP rule at 31 CFR 1020.220 expressly permits verifying identity by comparing customer details against a consumer reporting agency, public database, or other source. Parallel rules cover broker-dealers, mutual funds, and futures firms.

## Q2 What docless methods does FINTRAC accept in Canada?

Two are docless by design. The credit-file method verifies against a Canadian credit file at least three years old, and the dual-process method uses two independent reliable sources. Both are set out in FINTRAC's methods guidance under the PCMLTFA.

## Q3 Does docless verification stop synthetic identity fraud?

Database matching alone does not, because a matured synthetic profile can look plausible on paper. Biometrically Enriched verification counters it by requiring a live facial match against the authoritative source record. A fabricated identity has no such record to match, so the attacker has to defeat presentation attack detection rather than simply pass a data check.

## Q4 What happens to users who cannot be matched against a database?

They fall back automatically to document verification with biometric matching in the same flow. Thin-file, new-to-country, and young applicants stay onboardable, and nobody is turned away because a bureau file is missing.

## Q5 Can Shufti verify a mobile driver's licence (mDL)?

Yes, live today. Shufti verifies state-issued mDLs starting with California and Louisiana, returning issuer-signed attributes including age and address, with a live selfie matched against the licence portrait where proof of person is needed. Additional states and wallets activate on client demand through configuration.

## Q6 Does one integration cover both the US and Canada?

Yes. Shufti runs Passive, Active, and Biometrically Enriched verification, document verification across 240+ countries and territories, and AML screening through one API, with routing configured per market and per risk tier.

## REFERENCES

# Sources

- 01 FinCEN, Customer Identification Programs for banks, 31 CFR 1020.220.  
[ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-B/section-1020.220](https://ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-B/section-1020.220)

---

- 02 FINTRAC, Methods to verify the identity of persons and entities.  
[fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng](https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng)

---

- 03 NIST, SP 800-63-4 Digital Identity Guidelines, final, July 2025.  
[csrc.nist.gov/pubs/sp/800/63/4/final](https://csrc.nist.gov/pubs/sp/800/63/4/final)

---

- 04 NIST NCCoE, SP 1800-42A, Digital Identities, Mobile Driver's License, initial public draft, March 2026.  
[csrc.nist.gov/pubs/sp/1800/42/ipd](https://csrc.nist.gov/pubs/sp/1800/42/ipd)

---

- 05 FTC, Consumer Sentinel Network 2025 figures, testimony to the Joint Economic Committee, March 2026.  
[ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud](https://ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud)

---

- 06 FBI Internet Crime Complaint Center, 2025 Internet Crime Report.  
[ic3.gov/AnnualReport/Reports/2025\\_IC3Report.pdf](https://ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf)

---

- 07 Competition Bureau Canada, Fraud Prevention Month release with CAFC 2025 figures, March 2026.  
[canada.ca/en/competition-bureau/news/2026/03/fraud-prevention-month-to-bring-hidden-crime-into-the-spotlight.html](https://canada.ca/en/competition-bureau/news/2026/03/fraud-prevention-month-to-bring-hidden-crime-into-the-spotlight.html)

---

- 08 GAO, Synthetic Identity Fraud, GAO-24-106770, September 2024.  
[gao.gov/products/gao-24-106770](https://gao.gov/products/gao-24-106770)

---

- 09 FinCEN, Alert FIN-2024-Alert004 on deepfake media schemes, November 2024.  
[fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial](https://fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial)

---

- 10 FDIC, 2023 National Survey of Unbanked and Underbanked Households, November 2024.  
[fdic.gov/household-survey](https://fdic.gov/household-survey)

---

- 11 Payments Canada, Canadian Payment Methods and Trends 2025.  
[payments.ca/sites/default/files/PaymentsCanada\\_Canadian\\_Payment\\_Methods\\_and\\_Trends\\_2025\\_EN.pdf](https://payments.ca/sites/default/files/PaymentsCanada_Canadian_Payment_Methods_and_Trends_2025_EN.pdf)

---

- 12 TSA, REAL ID and mobile driver's licences.  
[tsa.gov/realid/realid-mobile-drivers-license-mdls](https://tsa.gov/realid/realid-mobile-drivers-license-mdls)

---

- 13 AAMVA, Mobile Driver License.  
[aamva.org/topics/mobile-driver-license](https://aamva.org/topics/mobile-driver-license)

---



TALK TO SHUFTI'S NORTH AMERICA TEAM

# The right next step is a conversation

Whether you are adding docless verification to an existing document flow, entering the US or Canadian market, or evaluating identity verification for the first time, Shufti's

North America team can map your products, risk tiers, and user base to the right verification configuration, with a clear view of which rails apply in each country and how AML screening and biometric-consent requirements are met alongside.

[Book a demo](#)

[SHUFTIPRO.COM](https://shuftipro.com)

[SUPPORT.SHUFTIPRO.COM](https://support.shuftipro.com)