

View in browser



Digital ID & Stolen Driver's License Fraud



SUMMARY

On September 8, 2026, **FINCEN**, NCUA and the federal banking agencies issued joint FAQs confirming that an unexpired, government-issued verifiable credential (VDC), such as a state-issued mobile driver's license, may qualify as government-issued identification under the Customer Identification Program (CIP) rule. A Financial Institution can accept certain digital IDs for CIP identification, provided it meets the applicable requirements.

However, there is an important distinction between a **government-issued, verifiable digital credential** and simply showing a picture or PDF of a driver's license on a phone.

A VDC is digitally signed by the issuing state and can be verified electronically; an image of a license cannot. The financial institution must still have a reasonable belief that it knows the account holder's true identity. The FAQs also note that indications of fraud in a government-issued electronic credential must be considered in forming that belief.

HOW FRAUD HAPPENS

- Stolen driver's-license information is obtained through identity theft, breaches, phishing or stolen wallets
- Fraudster creates a counterfeit physical ID or a digital representation of one
- Legitimate ID information is used to open accounts, obtain loans or establish digital banking access
- AI/deepfake technology may be used to defeat selfie, facial-match and liveness controls
- Fraudster exploits weaknesses between **online, branch and call-center authentication**

RED FLAGS

- ID information is valid, but applicant cannot be reliably authenticated as the legitimate owner
- Applicant presents a photo, screenshot or PDF of a license and represents it as a digital ID
- Digital credential fails signature, issuer, or revocation validation
- Multiple applications associated with the same ID, device, phone, email or address
- New device, IP, or geolocation inconsistent with applicant profile
- Facial mismatch, unusual selfie/liveness results or repeated verification failures
- Rapid account funding followed by ACH, wire, debit card or digital wallet activity
- Applicant unable to answer basic identity or account-history questions

KEY CONTROLS

Financial Institutions may wish to consider:

- ID authentication: document security features and barcode/data validation
- Person authentication: independent identity data verification, with facial comparison and liveness checks where appropriate
- Electronic validation of VDCs against the issuing authority's trust list, rather than visual inspection
- Confirming the CIP and related procedures have been updated before accepting VDCs in any channel
- Device, IP, behavioral and velocity analytics
- Detection of reused identity documents and applicant attributes across accounts
- Consistent controls across digital, branch and call-center channels
- Risk-based manual review before funding, loan disbursement, or high-risk access

- Step-up authentication for changes to credentials, devices, contact information, or transaction limits

RISK MITIGATION RESOURCES

- [Bronx resident pleads guilty to conspiracy targeting Credit Unions](#)
- [153 million driver's license scams may be on the dark web](#)
- Visit our [Fraud Prevention Center](#) to learn best practices on protecting against risk to your institution

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.

Stay ahead of fraud threats.
Access risk alerts, expert resources, the Let's Talk Fraud webinar series, and more — all in one hub.

Explore the Fraud Prevention Center

