After ID Verification Data Breach, FraudFighter Urges Businesses to Rethink Customer ID Storage

GLENDORA, CA, UNITED STATES, September 17, 2026 /EINPresswire.com/ -- FraudFighter™, a UVeritech, Inc. company, is urging businesses that scan government-issued identification to review how their identity-verification providers store, isolate and retain sensitive customer data following a recently disclosed security incident involving a major ID verification provider.

Earlier this month, a dark-web marketplace claimed to offer more than 153 million U.S. and Canadian driver's-license records, along with millions of other identity documents. Public reporting described some records as containing front and back document images as well as infrared and ultraviolet scans.
The identity-verification provider linked to the incident subsequently confirmed that an unauthorized third party may have accessed or copied certain customer information stored in its cloud environment. The provider said potentially affected information may include names and driver's-license or other government-issued identification numbers. The total number of individuals affected has not been publicly confirmed.

The incident is a stark reminder of a risk that many businesses accept without realizing it: every time a customer's driver's license or ID is scanned for age verification, rental, financing, or account opening, that data has to go somewhere. For businesses using cloud-dependent, third-party ID scanning services, "somewhere" often means a centralized, high-value database; the kind of target that made this breach possible in the first place.

"This breach isn't really about one vendor," said J.B. Dela Cruz, VP of Sales, FraudFighter. "It's a wake-up call for any business that hands a customer's ID to a third party without knowing exactly how, where, and for how long that data is stored. Businesses need to ask hard questions about their ID verification vendor's data architecture before the next breach happens, not after."

Businesses Should Review How Their ID Data Is Handled

Millions of consumers had their most sensitive identity documents exposed; data that can be used for identity theft, account takeover, and even physical safety risks for people who cannot afford to have their old address or appearance surface publicly, such as domestic violence survivors and individuals in witness protection. For the businesses that collected that ID data in

good faith, the fallout includes reputational damage, potential regulatory exposure under state data-breach notification laws, and a direct hit to customer trust.

Businesses in car rental, automotive sales, cannabis retail, financial services, gaming, and age-restricted retail; the industries most likely to scan a government ID at the counter; should be asking their current ID verification provider three questions right now:

1. Where is our customers' ID data actually stored, and for how long?
2. Is our data isolated from other customers', or pooled in a shared, high-value database?
3. Is our vendor independently audited (e.g., SOC 2 Type II); or just claiming to be secure?

FraudFighter Emphasizes Data Isolation And Customer-Controlled Retention

FraudFighter ID was built around a different principle: businesses need confidence that an ID is genuine and that the person presenting it is who they claim to be, not a permanent, centralized vault of every ID ever scanned.

- Customer data isolation. Each FraudFighter customer's data lives in a dedicated trust zone with unique encryption keys, so accounts are never pooled together in one shared database.
- Encryption at rest and in transit, on Microsoft Azure's “always-encrypted” infrastructure.
- Configurable data retention, including auto-delete rules, so businesses - not a third-party vendor - control how long ID data is kept.
- SOC 2 Type II certification, independently audited by Prescient Assurance under AICPA standards, with the audit report available to customers and prospects on request.
- Role-based access control so only the right people, at the right locations, can view sensitive scan data.
- On-site and mobile authentication options, including Desktop, Mobile, and WebID, so businesses aren't forced to route every ID scan through a single centralized cloud repository.

“Fake IDs and stolen identities are only half the fraud problem,” the company noted. “The other half is what happens to the real IDs after they're scanned. Businesses need a partner who treats their customers' data with the same seriousness they'd want for their own.”

Any business that scans, stores, or manually reviews government-issued IDs should treat this breach as a deadline, not a headline. FraudFighter is offering free consultations and 30-day trial programs to help businesses:

- Audit how their current ID verification process handles and stores sensitive data
- Deploy real-time ID authentication that flags forged, altered, or stolen identities at the point of transaction
- Add Risk Analysis data verification to catch identities that pass a visual check but fail a data cross-check
- Centralize oversight, access control, and compliance reporting through the FraudFighter Portal

Businesses reviewing their current identity-verification process can request a free consultation and 30-day trial at fraudfighter.com/contact or by calling (888) 664-9214.

About

FraudFighter™, a UVeritech, Inc. company, has delivered fraud prevention solutions to retailers, banks, casinos, rental agencies, and government offices for more than 25 years. Its FraudFighter ID platform combines device intelligence, machine-learning software, and cloud services to authenticate driver's licenses, passports, and other government IDs in real time, at the counter, on a mobile device, or remotely. FraudFighter is SOC 2 Type II certified and has more than 1 million units installed nationwide, trusted by organizations including Wells Fargo, Disneyland, Avis, Hertz, Nike, and T-Mobile. For more information, visit fraudfighter.com.

FraudFighter™
FraudFighter™ / UVeritech, Inc.
+1 888-664-9214
info@fraudfighter.com

This press release can be viewed online at: https://www.einpresswire.com/article/943000414

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.