EXCLUSIVE FROM

melissa

SECURING CREDIT UNIONS:

The Role of Advanced eIDV Technologies in Fraud Prevention

A few checks go a long way in securing businesses against fraud.

Fraud is a persistent threat to financial institutions, and credit unions are no exception. In recent times, the financial services sector has experienced a staggering 149% increase in suspected digital fraud attempts, showcasing the urgency to bolster security measures. Not only is fraud increasing in frequency, but its associated costs are also on the rise. Financial institutions now spend approximately $4.23 for every $1 lost to fraud, reflecting a significant hike from $3.64 in 2020. Amidst this growing concern, credit unions are witnessing a steady rise in membership, with the Credit Union National Association (CUNA) reporting an increase of 4.4 million new members between 2020 and 2021. As credit unions grapple with the challenge of balancing growth with security, adopting efficient and cost-effective fraud prevention measures becomes imperative.

The alarming surge in fraudulent activities at financial institutions places credit unions at significant risk, necessitating proactive measures to safeguard against evolving threats. Synthetic Identity Fraud (SIF), a particularly insidious form of fraud, involves the use of genuine personal information like valid Social Security numbers and birth dates combined with fabricated data, such as false addresses. Detecting such sophisticated fraud becomes especially challenging with outdated fraud-detection technologies. The rise of SIF coincides with exponential growth in credit union membership, highlighting the critical need for credit unions to adapt swiftly to changing threats. However, a complete overhaul of existing systems is both expensive and time-consuming. A far more straightforward and cost-effective means to achieving success in this pursuit involves integrating complementary solutions that work seamlessly with existing technologies.

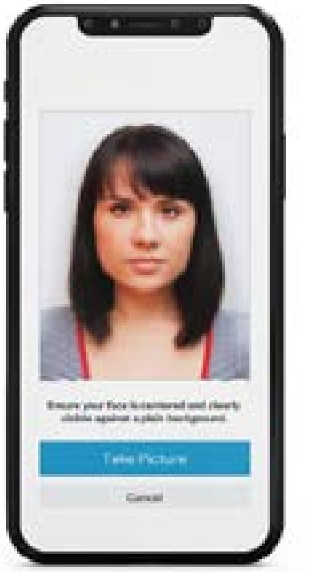
CRITICAL COMPONENTS OF AN EFFECTIVE SOLUTION

To effectively combat the escalating risk of fraud, credit unions need a comprehensive solution that incorporates eIDV (electronic identity verification) tools to cross check contact data in real time without negatively impacting the applicant's experience. Six crucial components of eIDV include geolocation, liveness checks, facial matching, document verification, address verification, and sanctions screening.

Utilizing **geolocation** data is instrumental in validating the authenticity of an applicant's claimed location. By cross-referencing the applicant's provided location data with their actual physical location obtained from geolocation services, credit unions can quickly identify potential discrepancies and red flags, prompting further investigation. Geolocation not only serves as a powerful fraud-detection tool but also enhances member experience by facilitating real-time and personalized notifications of nearby offers, adding value to the credit union's services.

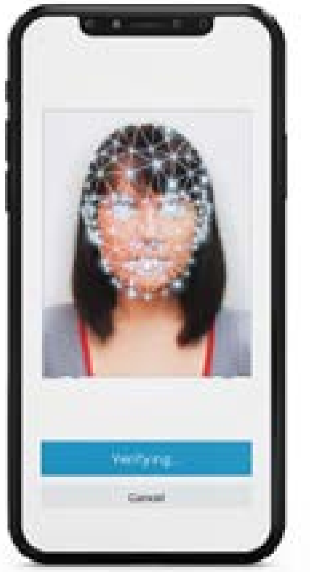
Distinguishing a genuine individual from a fraudster is essential in fraud prevention. **Liveness checks**, which come in two forms – active and passive – ensure that the person interacting with the system is a real, live individual. While active checks require specific actions like blinking or facial gestures to confirm liveliness, passive checks analyze various factors such as light exposure and micro movements to achieve the same result. Passive checks offer a smoother user experience, minimizing friction while maintaining high security standards.

Facial matching involves comparing the facial features captured in a real-time selfie during the onboarding process with those on the government-issued identification document provided by the applicant. Advanced algorithms rapidly determine if the images match, allowing for quick identification of any discrepancies. This technology is essential in preventing identity fraud and maintaining a high level of security during the onboarding process.



Ensure your face is centered and clearly visible against a plain background

Liveness checks

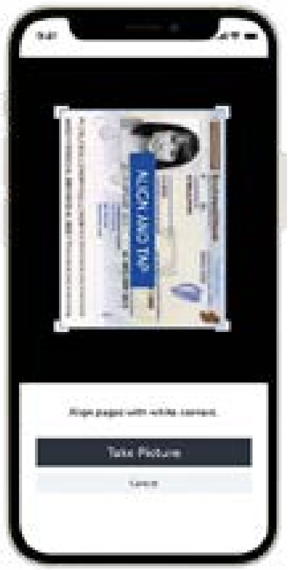


Facial matching

The applicant typically provides critical identity documents, such as a driver's license, during the application process. **Document verification** analyzes the authenticity of these documents in real time by checking for watermarks, file formats, and other security features, ensuring their legitimacy. The technology also extracts relevant data, like the applicant's address, for cross-verification and comprehensive identity validation.

Verifying the accuracy and authenticity of the applicant's address is a crucial step in fraud prevention. Credit unions can detect discrepancies and potentially fraudulent activities by confirming the provided name and address against various databases. This **address verification** element enhances fraud prevention while simplifying the customer journey, eliminating the need for additional proof-of-address documentation.

[1] SOURCE: https://www.sba.gov/article/2023/06/27/us-small-business-administration-releases-report-anti-fraud-control-measures-pandemic-relief



Document verification

eIDV tools also support **sanctions screening** and **compliance operations**. Compliance is dependent on current, relevant data from multiple sources – a range of data streams containing billions of global contact records. Useful data points are accessed from government agencies, credit bureaus, and data list vendors, as well as international watchlist entities tasked with combatting the funding of narcotics and terrorism. Data tools can consolidate watchlist screening, verifying players against such lists as PEP (Politically Exposed Persons), SDN (Specially Designated Nationals and Blocked Persons), and additional lists from OFAC (the Office of Foreign Assets Controls) and other economic sanctions entities across the U.S., U.K., and E.U. **Federally insured credit unions are required to enforce these sanctions** and should maintain a current list of these prohibited individuals and countries, and compare their members, new members, and account transactions against the list, blocking all accounts and transactions with the prohibited entities.

IMPLEMENTING A COMPREHENSIVE SOLUTION

To effectively counter fraud and maintain a seamless onboarding experience, credit unions must integrate these critical eIDV components into a cohesive solution. Solution deployment involves a structured approach that balances security and user convenience.

Initiating the application process should be simple for the prospective member. By offering the ability to kickstart the application process online, the organization caters to the growing demand for digital experiences. Accessibility through multiple devices, including smartphones and computers, accommodates varying member preferences.

Capturing essential documents is necessary, but don't make it a chore. By prompting applicants to capture images of their government-issued identification documents (i.e., driver's license, passports), during the application process, the financial institution keeps the process moving. Images are securely uploaded to the credit union application for verification.

> **"Financial institutions spend $4.23 for every $1 lost to fraud"**

Real-time data verification streamlines the application process. Advanced technology rapidly processes the captured images, employing geolocation data, liveness checks, facial matching, and document verification to assess their authenticity and accuracy. Simultaneously, the system cross-references the provided information with various datasets, validating the identity in real-time.

Automated approval and follow up can speed member onboarding or raise concerns. Based on the outcomes of the real-time verifications, the membership application is either automatically approved, providing a swift and frictionless experience for the member, or flagged for further review if potential security issues are identified. In the latter case, credit union staff can investigate the concerns following established protocols, ensuring comprehensive scrutiny of questionable applications.

TACKLING THE ESCALATING THREAT

As credit unions grapple with the increasing challenges posed by fraudsters, adopting advanced technology becomes imperative to bolster security and maintain a positive member experience. The evolving landscape of fraud necessitates proactive measures that keep pace with the sophistication of modern-day criminals. Integrating complementary eIDV technologies that encompass geolocation, liveness checks, facial matching, document verification, and address verification offers a cost-effective approach to fortify credit union security without the need for a complete overhaul.

By effectively leveraging these crucial components, credit unions can mitigate risks, provide robust fraud prevention, and enhance member experiences, ultimately fueling future growth and prosperity.

ABOUT THE AUTHOR

Authored by *Bud Walker*, Chief Information Officer, Melissa. Bud manages the strategic vision and next-generation capabilities of Melissa's data quality tools and services. Connect with Bud at bud.walker@melissa.com or LinkedIn.