melissa

A **MELISSA** WHITEPAPER

Stemming the Tide on the New Era of Fraud

A recent report shows a 149% increase in global digital fraud attempts targeting financial services.[1] Here's how credit unions can leverage technology to close security vulnerabilities.

By Nicki Howell

TABLE OF CONTENTS

STEMMING THE TIDE ON THE NEW ERA OF FRAUD

- Credit union membership is steadily growing across the country at a time when fraud risk is escalating.
- Older technologies for verifying identity often come up short, and bad actors slip through the cracks.
- Rip-and-replace solutions are expensive and time-consuming, but complementary solutions help save money by working with existing technologies.
- A solution should include five critical components: geolocation, liveness checks, facial matching, document verification, and address verification.

INTRODUCTION

Fraudsters are targeting financial services organizations at an alarming rate, and credit unions are no exception. A report published by TransUnion found a 149% increase in suspected digital fraud attempts in the financial services sector.[1] At the same time, the cost of fraud is steadily rising. Research shows that for every $1 of fraud loss, financial institutions spend $4.23, an increase from just $3.64 in 2020.[2]

A considerable threat to credit unions is Synthetic Identity Fraud (SIF). It uses various types of real information, such as valid Social Security numbers and birth dates, along with falsified data like fake addresses. Spotting this type of fraud isn't always straightforward with older fraud-detection technologies.

Additionally, the rise of SIF is happening at a time when credit union membership is steadily expanding. CUNA reported an increase of 4.4 million new members between 2020 and 2021, and that growth is expected to continue.[3] Keeping up with fast-changing threats is a priority for credit unions, but a rip-and-replace approach is expensive and time consuming. That's why many are considering an alternative: adding complementary solutions to close security gaps.

However, before considering this type of solution, it's essential to understand what technologies are most effective for closing down security vulnerabilities. This whitepaper will cover the most important capabilities, including geolocation, liveness checks, facial matching, document verification, and address verification.

FRAUD IS HAPPENING MORE OFTEN – AND THE COST IS RISING

Global digital fraud attempts targeting financial services increased by 149%[1]

Every $1 of fraud costs credit unions $4.232

The Cost of fraud has risen 16.2% since 2020 in the United States[2]

Source: Annual LexisNexis Risk Solutions Report Finds Fraud Costs up to 22.4% from Pre-Pandemic Levels Across U.S. and Canadian Financial Services Firms (prnewswire.com)

1. "Fraudsters Targeting Financial Services More Than Any Other Industry in 2021," Credit Union Times, June 3, 2021.
2. A "Annual LexisNexis Risk Solutions Report Finds Fraud Costs up to 22.4% from Pre-Pandemic Levels Across U.S. and Canadian Financial Services Firms," Cision PR Newswire, November 16, 2022
3. "Credit Unions Mark Unprecedented Growth," PYMNTS, January 3, 2022.

LEVERAGING GEOLOCATION DATA TO FERRET OUT FRAUDSTERS

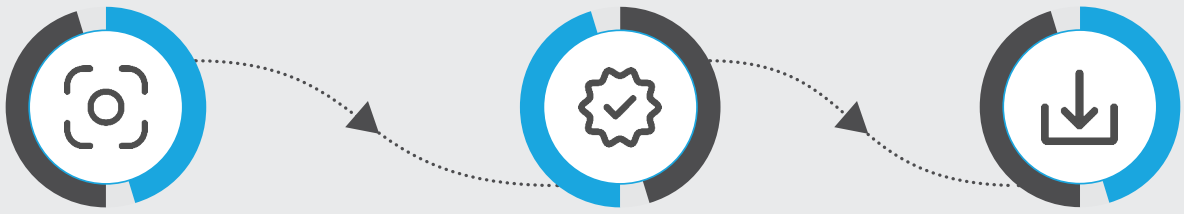
Preventing fraud requires credit unions to uncover the true identity of applicants during the onboarding process. For example, if an applicant claims to live in New York, and you discover through geolocation their actual location is 7,000 miles away, that's a red flag. An alert allows your employees to complete additional follow-ups to investigate the risks.

Geolocation is a tool that makes tapping into this intelligence possible. Many smartphone users enable location services on their devices. When the applicant completes the onboarding process, geolocation taps into that information to verify a person's physical location is consistent with their application data. As a result, you can spot discrepancies for further investigation.

However, ensure that you select a solution that can convert U.S., Canadian, and other international postal addresses in real time to determine the applicant's precise latitude and longitude coordinates. This capability allows you to tap into precise data and match that data more easily with the application information.

Credit unions using geolocation can also harness that data to improve the member experience. An example is notifying members of nearby offers when the person is in a geofenced area. Providing real-time and personalized experiences enables credit unions to offer more member value.

The 3 Steps for Digital Identity Verification



STEP-1

CAPTURE

Prospective members capture images of their ID documents anytime, anywhere in seconds.

STEP-2

VERIFY

ID documents are verified using biometrics, document verification, and address checks.

STEP-3

STORE

Comprehensive customer due dilligence reports are generated and securely stored.

TAPPING INTO "LIVENESS" CHECKS TO SPOT INCONSISTENCIES

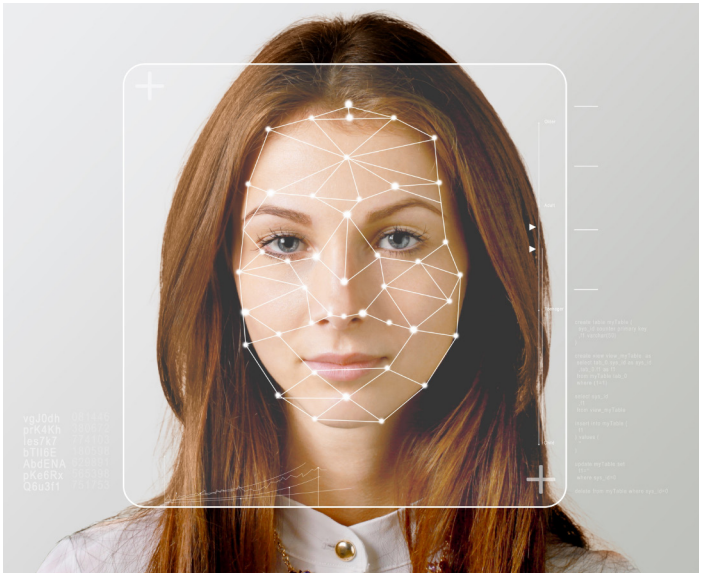
A bad actor might use a real Social Security number, birth date, and other information to manufacture a fake ID. The fraudster then uses the fake ID to attempt to open a credit union membership. At first glance, it can be difficult to distinguish between a legitimate government ID and a fake one, especially when safety measures vary from state to state.

Advanced identification verification capabilities allow credit unions to complete "liveness" checks during onboarding. This ensures the person submitting the information is a real live person – and not a fraudster. Two types of liveness checks exist, including:

- **Active liveness check:** The active check leverages software that detects factors such as facial gestures, eye movement, or lip movement. The safety measure requires a user to complete some type of action to confirm they're real, such as blinking. As a result, an active check takes longer than the second option, which is a passive check.
- **Passive liveness check:** The passive check requires no additional action from the applicant. Instead, the technology determines liveness using other factors, such as light exposure, micro movement detection, depth measurement, and more.

Both active and passive checks can help credit unions identify fraud, but there is one main difference between them. A passive check creates far less friction for the member experience, a critical factor when you are trying to compete on experience and offer more member value.

IMPROVING ACCURACY WITH FACIAL MATCHING



Liveness checks and facial matching go hand in hand when preventing fraud. During the identity verification process, facial matching compares the face from the identity documentation the applicant provides to the face of the person completing the process.

For example, a potential credit union member might apply for a new membership. First, the member takes a real-time photo of their driver's license. Additionally, they take a selfie so the technology can match the real live person using facial matching – comparing the identification to a picture the person takes of themself.

A comparison algorithm is used to quickly determine whether the selfie and photo on the government-issued ID match, and can distinguish changes such as hair, makeup, and hairstyle. If there isn't a match, the application is passed to a human to process and rule out fraud.

STREAMLINING AND IMPROVING DOCUMENT VERIFICATION ACCURACY

During a new membership application, a person provides important documents, such as a driver's license, to verify their identity. The documents are uploaded into a mobile application in most cases, and during that upload, critical data is captured. With that information, you can take a deeper dive into the verification process in real time.

The technology will often check the document to make sure it's legit. In addition, the tool refers to many file formats, watermarks, and other details that issuing institutions created to protect the sanctity of the documents and make them difficult to forge.

The technology also extracts data from the document, such as the applicant's address, and cross-checks it to ensure the information is correct. And, of course, you have all the other tools working in the background, like facial recognition and biometrics (liveness checks, facial matching, and more) to be absolutely certain the applicant is legit.

DIGITAL IDENTITY VERIFICATION: BUILD OR BUY?

As credit unions weigh options for improving identity verification, they have two options: build it or buy it.

- **Building a solution:** is attractive because it's customized. Yet credit unions often run into challenges, one being expense. But there's also the challenge of tapping into all the critical data sources to verify identity. For example, how do you organize and connect to USPS address sets? How can you find credit data, utility company data, and more and pull that into a comprehensive solution? These considerations can make the "build" option expensive and time consuming.
- **Buying a prebuilt solution:** A prebuilt solution is "plug and play" and can integrate with your existing technologies. Additionally, since it's been used by other credit unions, the bugs you might encounter with a build-it-yourself solution are worked out. As you consider options, remember that you never want to spend more than you can save. Ensure that a potential solution provider can show you ROI.

VERIFYING ADDRESS DATA AND INFORMATION

The fraudster who pulls together many bits of information, some real and some fictitious, might use a real Social Security number and a real birth date, and then make up an address. And here is where you have an opportunity to catch them.

A solution that goes deep with address verification provides an additional level of protection, ensuring the individual's name and address are extracted from onboarding information and verified against multiple databases to ensure the address is real.

This step helps provide stronger fraud prevention while simplifying the customer journey, with no need for the customer to submit separate proof-of-address documents.

ONBOARDING FRAUD PREVENTION IN ACTION – PULLING IT ALL TOGETHER

Credit unions considering a complementary solution to level up onboarding fraud protection should ensure the technology includes the five most critical areas: geolocation, liveness check, facial matching, document verification, and address verification. These capabilities work synergistically to ensure fraud doesn't slip through the cracks. Here's an example of how this might come together for a credit union.

1. **The member completes an application online.** An increasing number of members want online and digital experiences, so the credit union allows them to launch the process from their computer or smartphone or other mobile device.

2. **The member is prompted to take a picture of the front and back of their driver's license,** passport, or other qualifying government-issued ID. The member uploads this into the credit union application.

3. **The technology works in real time to capture the various data sets.** It checks for liveness, document authenticity, address verification, and more to ensure the ID is valid. It answers questions such as: Does the name match the address? Is the cell phone a live, callable number? Does the geolocation align with the application? This data and more are checked in real time.

4. **The technology verifies the applicant's identity.** After being run through all the checks, the membership application is approved. The member is happy because it was fast, easy, and online. The credit union is happy because the entire process was automated, and the member's first interaction was excellent, making it easier for the credit union to cross-sell more business in the future.

5. **An alternative scenario – potential security issues are spotted,** and the application is referred to the credit union. A staff member follows up using internal processes to investigate possible security issues. However, with so many applications approved automatically, credit union employees have more time to handle special cases.

CONCLUSION

It's difficult to predict the future, but if the past is any indicator, we know this: As credit unions get more advanced in fighting fraudsters, criminals will also level up their tactics. Staying ahead of threats requires credit unions to use technology that keeps pace with new and advanced threats.

Implementing technologies that complement existing fraud protection rather than rebuilding from the ground up enables you to leverage what you already have without needing to rip and replace. But to succeed, you want to ensure that any complementary technology has the most important capabilities. This will help mitigate risk, so fewer criminals will slip through the cracks during onboarding – and you'll simultaneously build positive member experiences, encouraging future growth.

melissa

www.melissa.com

About Melissa

Melissa is a leading provider of data quality, identity verification and address management solutions. Melissa helps businesses win and retain customers, validate and correct contact details, optimise their marketing ROI and manage risk. Since 1985, Melissa has been a trusted partner for key industries like retail, education, healthcare, insurance, finance, and government. For more information visit www.melissa.com or call 1-800-Melissa.

US

22382 Avenida Empresa
Rancho Santa Margarita, CA 92688-2112

800 MELISSA (635 4772)

GERMANY

+49 (0) 221 97 58 92 40

CANADA

800 635 4772

INDIA

+91 (0)80 4854 0142

UK

+44 (0)20 7718 0070

AUSTRALIA

+61 02 8091 6000

SINGAPORE

+65 8 2997442