melissa

A **MELISSA** EBOOK

Enhancing Electronic ID Verification Through Contact Data Quality

An insightful eBook on how contact data quality is the key to eIDV enhancement.

TABLE OF CONTENTS

ABOUT THIS EBOOK

This eBook delves into how improving contact data quality can significantly bolster electronic ID verification providers by streamlining operations and enhancing the user experience.

Accurate and up-to-date contact data underpins advanced verification features, enabling providers to detect fraudulent activities more effectively, personalise user interactions, and reduce operational inefficiencies. This not only improves the overall efficiency of the verification process but also enhances customer satisfaction by delivering a more responsive and personalised experience.

By prioritising data quality, eIDV providers can position themselves as leaders in the market, offering secure, compliant, and user-friendly services that meet the evolving demands of the digital age and adapting to new market needs.

BUYERS NEEDS ARE EVOLVING WHILE VENDOR COMPETITION IS INCREASING

As the market for identity verification solutions evolves, buyers' needs are expanding, all while competition among vendors intensifies. This competitive environment is driving vendors to differentiate themselves by offering innovative and forward-looking features that go beyond the current landscape. While on the other side, end-user organisations face challenges in selecting a vendor from a crowded marketplace, often defaulting to those with regional experience. To counter this, vendors are incorporating advanced capabilities to stand out and facilitate expansion into new regions and use cases. These additional features include:

- **Data-Centric Identity Affirmation Signals:** Vendors are increasingly using data extracted from identity documents and cross-referencing it with other sources, such as identity graphs, credit bureaus, or government authorities, to strengthen identity verification.
- **Adjacent Authentication Capabilities:** Biometric authentication, particularly face and voice biometrics, is being offered by some vendors, using the initial identity verification event as a trust anchor. This is especially useful in scenarios like remote hiring or account recovery.
- **Low-Code Integration:** Solutions that offer easy integration, such as low-code platforms or out-of-the-box solutions that can be operational within minutes, are becoming more popular.

Gartner states that historically, identity verification was primarily used during customer onboarding to meet KYC requirements. However, its use has expanded significantly in the past 12 to 18 months for an ever-broader range of use cases [1].

Government agencies are now using identity verification to prevent fraud in benefits claims, while marketplace and gig economy platforms employ it to ensure trust and safety among users and human resources teams are leveraging these solutions to streamline remote hiring processes [1].

Notably, there is growing interest in using identity verification for security purposes, particularly in credentialing and account recovery processes. This is especially relevant when multifactor authentication (MFA) is not feasible, such as when a user has lost their device, highlighting the importance of identity verification in enhancing security and reducing the operational burden on IT help desks [1].

[1] HTTPS://JUMIO.PATHFACTORY.COM/C/JUMIO-GARTNER-2023?X=ZXBNOK&LB_STUART.MCPHERSON@MELISSA.COM&UTM_SOURCE=PATHFACTORY&UTM_MEDIUM=WEBSITE&UTM_CAMPAIGN=2023+GARTNER+MARKET+GUIDE+FOR+IDENTITY+VERIFICATION

IMPLEMENTING CONTACT DATA QUALITY IN THE eIDV PROCESS

As electronic identity verification (eIDV) services become increasingly essential in various industries, the accuracy of contact data has emerged as a critical factor for providers aiming to differentiate themselves in a competitive market. We have found that the quality of contact data is foundational to the effectiveness of eIDV processes, influencing everything from fraud prevention to mitigating simple ID checks where more advanced techniques like biometrics or liveness authentication may not be necessary.

As a starting point, when a customer's contact information, such as address, email, and phone number, are accurate, the verification process becomes more reliable. This accuracy ensures that the system can cross-reference the provided information against official databases or other authoritative sources without discrepancies that could lead to false positives or negatives [2][3].

In saying this, fraudsters often exploit inaccuracies in contact data to create false identities or manipulate existing ones. By maintaining clean and accurate data, eIDV systems can more effectively detect suspicious activities and prevent fraud. For example, discrepancies in a user's phone or email information, or an address linked to multiple identities, could serve as red flags triggering additional scrutiny. This basic yet crucial capability is especially important as identity-related fraud becomes more sophisticated. However, some ID vendors may overlook this step, placing too much emphasis on advanced technological solutions [2][3].

Beyond the technical aspects of verification, accurate contact data also supports personalised user experiences and operational efficiency.

When eIDV systems have access to reliable data, they can tailor interactions with users, making the verification process more seamless and user-friendly. For example, pre-populated forms, accurate address suggestions, and real-time contact data verification can enhance the onboarding experience, reducing friction and increasing the likelihood of successful transactions.

Moreover, obtaining clean data minimises the time spent resolving verification issues and reprocessing applications due to inaccuracies. This boosts operational efficiency and reduces costs related to data correction and customer support. [2][3].

[2] HTTPS://WWW.FINEXTRA.COM/BLOGPOSTING/23131/DATA-QUALITY-IS-KEY-FOR-EFFECTIVE-ID-VERIFICATION

[3] HTTPS://CHAINSTOREAGE.COM/MELISSA-QUALITY-FOUNDATIONAL-DATA-KEY-TO-DIGITAL-IDENTITY-VERIFICATION

ADDRESS INTELLIGENCE: A FUNDAMENTAL PILLAR

Address verification is increasingly recognised as the cornerstone of contact data quality, serving as a critical enhancement for many electronic identity verification (eIDV) vendors. In a digital-first world where remote interactions are increasingly common, verifying the accuracy and legitimacy of an individual's address should be the first step in any identity-related process [2].

Ensuring data accuracy and consistency through address validation reduces errors caused by typos or incorrect input, leading to more reliable identity verification. By standardising addresses across different databases, it also maintains consistency, making it easier to match and verify identities across multiple sources.

Address verification is also vital for fraud prevention, for instance, discrepancies between a claimed address and official records can be significant red flags for potential fraud. These inconsistencies may indicate attempts to mislead or manipulate identity information, prompting further investigation. This level of vigilance is crucial in preventing activities like insurance scams, where fraudulent claims can lead to significant financial losses, or identity theft, where stolen identities are used for illicit purposes. By catching these discrepancies early, eIDV systems can help mitigate risks, protect both businesses and individuals from fraud, and ensure that only legitimate users are granted access to services. This proactive approach not only enhances security but also fosters trust in the verification process [5].

Regulatory compliance is another critical area where address verification plays a key role. It ensures that the address information provided by customers meets Know Your Customer (KYC) and Anti-Money Laundering (AML) regulatory standards, thereby reducing the risk of non-compliance. Accurate address information is essential for monitoring and reporting suspicious activities, further strengthening the integrity of any eIDV process.

Tools like address autocomplete or lookup services are invaluable when customers complete contact forms on small mobile screens, where mistakes are more likely. By reducing the number of keystrokes required—by up to 81%—these tools speed up the onboarding process, decreasing the likelihood of incomplete applications or abandoned purchases. They also support ID verification by delivering real-time address verification [2].

Find or Check a Postcode

E1 03A

Flat 1, Oxford House, Black Street, London, Middlesex, E1 03A

Flat 2, Oxford House, Black Street, London, Middlesex, E1 03A

Flat 3, Oxford House, Black Street, London, Middlesex, E1 03A

Flat 4, Oxford House, Black Street, London, Middlesex, E1 03A

[2] HTTPS://WW.FINEXTRA.COM/BLOGPOSTING/23131/DATA-QUALITY-IS-KEY-FOR-EFFECTIVE-ID-VERIFICATION
[4] HTTPS://WWW.TRULIOO.COM/BLOG/IDENTITY-VERIFICATION/VERIFYING-ADDRESSES
[5] HTTPS://WWW.INCOGNIA.COM/BLOG/ADDRESS-VALIDATION-VS-ADDRESS-VERIFICATION

TAKING VERIFICATION TO NEW HEIGHTS WITH GEOCODING

Geocoding, the process of converting physical addresses into geographic coordinates, offers a sophisticated tool that goes beyond traditional address verification methods by providing an unprecedented level of precision. By pinpointing the exact location of an address, geocoding ensures that the data organisations rely on is both accurate and reliable, reducing errors associated with ambiguous or incorrect addresses and strengthening the overall integrity of the electronic identity verification (eIDV) process [4].

Additionally, geocoding enhances fraud detection by enabling the identification of non-residential addresses, such as PO boxes or commercial properties, which are often used to obscure true locations. The ability to cross-verify geocoded addresses with other data sources further bolsters security, providing a critical layer of protection in today's increasingly digital and interconnected world.

We have highlighted four key dimensions on how geocoding enrichment adds significant value to electronic identity verification (eIDV):

1. Enhanced Accuracy in Address Verification

By converting a physical address into geographic coordinates, geocoding provides a more precise identification of a location. This precision minimises errors related to ambiguous or incorrectly entered addresses, ensuring that the address used in eIDV corresponds to an exact point on a map [5].

This also plays a crucial role in verifying that the address exists in the real world, being especially important in scenarios where fabricated or incorrect addresses might be provided, as it confirms the address is tied to a legitimate location.

2. Improved Fraud Detection

With geocoding's pinpoint capabilities, it can distinguish between residential addresses, commercial properties, and PO boxes. This capability is essential for detecting attempts to use non-residential addresses, which could be indicative of fraudulent activity or attempts to obscure the true location [6].

Geocoding also allows for cross-referencing an address with other data sources, such as utility records or property databases. This additional layer of verification helps confirm the legitimacy of the address and can flag discrepancies that might suggest fraudulent behaviour.

3. Geospatial Risk Assessment

Geocoding enables businesses to assess risk based on the geographical location of an address. For instance, certain areas may have higher rates of fraud or may be subject to specific regulatory scrutiny, allowing companies to apply more stringent verification or additional checks in those regions.

Another factor to take into consideration is distance and proximity checks, by understanding the geographic relationships between addresses, businesses can perform these checks that are useful for identifying suspicious patterns, such as inconsistencies between a claimed residential address and other known locations, like billing addresses or workplaces.

4. Improved Compliance with Local Regulations

Jurisdictional Verification uses geocoding to ensures that an address falls within a particular jurisdiction, which is crucial for complying with local regulations. This is particularly important for industries that operate across multiple regions or countries, where different legal requirements may apply.

This is also necessary for applying the correct tax rates and ensuring adherence to regional laws. For instance, tax rates can vary significantly even within small geographic areas, and precise geocoding ensures the correct rates are applied based on the exact location [4][5].

[4] HTTPS://MEDIUM.COM/@TEJASWINIG/THE-ULTIMATE-GUIDE-TO-GEOCODING-EVERYTHING-YOU-NEED-TO-KNOW-53832075F76B

[5] HTTPS://WWW.MELISSA.COM/ADDRESS-EXPERTS/WHAT-IS-GEOCODING

[6] HTTPS://TRAVELTIME.COM/BLOG/WHY-GEOCODE

PHONE AND EMAIL VERIFICATION: SIMPLE & EFFECTIVE

As electronic identity verification (eIDV) systems become increasingly sophisticated, the role of phone and email verification has emerged as an essential component to a comprehensive verification process. Especially when it comes to implementing additional features like fraud detection signals, helping organisations identify and mitigate potentially fraudulent activities early on.

Email verification involves analysing various factors such as the age and history of the email address, the domain and syntax, and whether the email is disposable or temporary. By assessing if the email first even exists then checking those various elements, organisations can identify high-risk indicators, such as newly created or poorly formatted email addresses, which are often used by fraudsters. Additionally, monitoring the activity and reputation associated with an email address can reveal whether it has been flagged for suspicious behaviour or as been blacklisted, further aiding in the detection of potential fraud. The association of a single email with multiple accounts can also signal fraudulent schemes, such as bonus abuse or account farming, allowing organisations to take preventive measures.

Phone verification or phone intelligence, similarly, plays a critical role in fraud detection. By verifying the type and carrier of the phone number, organisations can identify high-risk numbers, such as those associated with VoIP services, which are commonly used in fraudulent activities. Checking the validity, activity, and geolocation of a phone number ensures that it is not only functional but also consistent with the user's claimed location. Discrepancies in geolocation can signal attempts to mask true locations, such as when fraudsters use VPNs. Like with email, a single phone number linked to multiple accounts can indicate fraudulent behaviour, enabling early intervention.

Together, email and phone verification contribute to enhanced security by filtering out fake or high-risk contact information, improving the overall accuracy of the eIDV process. These methods support regulatory compliance, particularly with Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements, by ensuring that organisations maintain up-to-date and accurate contact records [2].

[2] HTTPS://WW.FINEXTRA.COM/BLOGPOSTING/23131/DATA-QUALITY-IS-KEY-FOR-EFFECTIVE-ID-VERIFICATION

IP LOCATION: A STRATEGIC ASSET IN THE VERIFICATION PROCESS

IP location has increasingly been recognised as a strategic asset in electronic identity verification (eIDV), serving as another prominent fraud detection signal, and adding significant value to various aspects of digital interactions.

We have highlighted 3 key areas where IP location can add value are:

Fraud Detection: By identifying discrepancies between a user's claimed location and their actual IP-derived location. This helps in flagging potential fraud, particularly when there is a mismatch in geographical regions. High-risk IP locations, such as those associated with proxy servers, VPNs, or regions with elevated cybercrime, are automatically flagged, allowing for preventive measures like blocking access or requiring additional verification. Real-time monitoring of IP locations further strengthens security by enabling immediate detection and response to suspicious activities, such as multiple logins from different locations within a short time [7][8][9].

Regulatory Compliance: This is another critical area where IP location analysis proves invaluable. It ensures adherence to regional laws, including data residency requirements, by verifying that user data is stored and processed within permitted geographical regions. This is crucial for complying with anti-money laundering (AML), counter-terrorism financing (CTF) regulations, and data protection laws like the General Data Protection Regulation (GDPR). By identifying users' locations, organisations can ensure that their data handling practices meet regulatory standards, thereby avoiding legal repercussions [7][8].

Improved User Experience: IP location analysis significantly enhances the user experience in electronic identity verification (eIDV) processes by enabling the delivery of personalised and localised content, such as displaying the correct language, currency, and region-specific information. This makes digital interactions more relevant and accessible. Additionally, IP location streamlines the verification process by pre-filling location-based information, reducing user effort, minimising friction, and speeding up the overall process. Moreover, it allows eIDV systems to implement context-aware security, simplifying verification for logins from familiar locations while applying additional checks for unfamiliar or high-risk areas [7][8].

[7] HTTPS://GEOTARGETLY.COM/BLOG/CAN-CREDIT-CARD-FRAUD-BE-MINIMISED-WITH-IP-GEOLOCATION
[8] HTTPS://FINGERPRINT.COM/BLOG/WHAT-IS-IP-GEOLOCATION/
[9] HTTPS://WWW.TRULIOO.COM/BLOG/PROOF-OF-ADDRESS

CONCLUSION

This ebook highlights that electronic identity verification processes hinge on the accuracy and quality of contact data. Clean, reliable data not only enhances fraud detection but also improves user experience and operational efficiency. This is a vital aspect as the identity verification market evolves with both vendors and end-user organisations facing unique challenges and opportunities.

For vendors, the pressure to innovate, differentiate and adapt to buyer needs is greater than ever. With the competitive landscape demands going beyond the current market standard this means that offering extra capabilities that address emerging needs of their customers and prospects is key.

To stand out in a crowded marketplace, and also expand into new regions and markets with confidence, vendors need to undertake a number of steps. These include incorporating immersive advancements like enhanced biometrics and low code/out of the box solutions, refining fundamental processes to achieve data integrity such as address verification, phone and email validation, and IP location analysis.

melissa

www.melissa.com/uk

Speak to a Specialist

About Melissa

Melissa is a leading provider of data quality, identity verification and address management solutions. Melissa helps buisnesses 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. Fot more information visit www.melissa.com/uk or call +44 (0)20 77180070.

UK

Floor 37, 1 Canada Square
Canary Wharf, London
E14 5AA, United Kingdom

Info.uk@melissa.com
+44 (0)20 7718 0070

U.S.
1 800 MELISSA (635 4772)

CANADA
1 800 635 4772

INDIA
+91 (0)80 4854 0142

GERMANY
+49 (0) 221 97 58 92 40

AUSTRALIA
+61 02 8091 6000

SINGAPORE
+65 8 2997442

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

HIPAA COMPLIANT

Crown Commercial Service *Supplier*

ico. Information Commissioner's Office REGISTERED