Aité PARTNER. ADVISOR. CATALYST.

Digital Identity Verification: Convenient and Compliant

SEPTEMBER 2017

Prepared for:

Mitek

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

Digital Identity Verification: Convenient and Compliant, commissioned by Mitek and produced by Aite Group, describes the many benefits of using automated processes to verify identities for digital account opening, loans, and payments.

Key takeaways from the paper include the following:

- Identity crimes, such as application fraud and account takeover (ATO), are growing rapidly in the post-EMV market in the U.S.
- Digital identity verification can address these threats by capturing and verifying the authenticity of identity documents and by verifying that the person submitting the document is the legitimate customer by taking a selfie and comparing it to the photo on the identity document when applying for a new account or accessing existing accounts.
- Capturing and validating identity documents electronically can assist with Know Your Customer (KYC) regulatory compliance requirements as well as anti-money laundering (AML) requirements for payments.
- Verifying identity documents can assist with combatting organized fraud rings' attempts to commit application fraud and ATO fraud schemes.
- Submitting an application for a new account or loan and verifying identity documents concurrently transforms this to a one-step process, which is simpler and more convenient for the customer, leading to higher levels of customer satisfaction.
- Capturing trailing documents digitally for proof of address or other required information streamlines the account opening process, thus improving the customer experience.

INTRODUCTION

The world is changing rapidly, and consumers spend more time online than ever before. Many people won't leave home without their mobile devices, and they are demanding expanded capabilities on those devices. As more consumers apply for new accounts, loans, and credit cards, and make payments via mobile devices, the risk of fraud increases. Financial institutions (FIs) are facing more threats via the digital channels than ever before; research shows that fraudulent applications are eight times higher online than in a branch.[1] In order to enjoy the financial benefits of moving more activity from physical locations to the digital channels, it is imperative that financial services firms be able to identify applicants and authenticate returning customers to negate the organized fraud threats and meet the regulatory requirements associated with AML legislation in the digital channels.

Identity document verification can assist FIs in many ways by capturing the content of the documents and validating the documents. This white paper will explore the many benefits financial services companies can derive from using a document authentication solution—fraud reduction, regulatory compliance, an exceptional customer experience, and improved operational efficiency.

METHODOLOGY

This white paper contains analysis from ongoing, in-depth Aite Group discussions with senior fraud and business line executives at global FIs, payment providers, and online lenders, as well as reference calls with Mitek clients.

1. See Aite Group's report *Application Fraud Rising as Breaches Fan the Flames*, March 2016.

DIGITAL IDENTITY VERIFICATION

In 1993, a Peter Steiner cartoon[2] published in the New Yorker became famous. The image of a dog on a computer with an aside to his doggie friend saying, "On the Internet, nobody knows you're a dog," was truly prescient. In the years since, the ability for people to misrepresent themselves online has become increasingly evident with fraudsters using stolen and completely fabricated identities for many purposes. The use of carefully nurtured synthetic identities makes it challenging for financial services firms to differentiate between them and real human beings during the application stage for new demand deposit accounts (DDAs), credit cards, or loans. Being able to determine whether your true customer is accessing his account or moving funds is also increasingly difficult as ATO attempts grow rapidly.

Long gone are the days when people recognized one another by face and primarily conducted business in person. As fraud attempts continue to proliferate, it is increasingly important for financial services firms to implement new methods of determining the identity of the individual on the other side of the digital device.

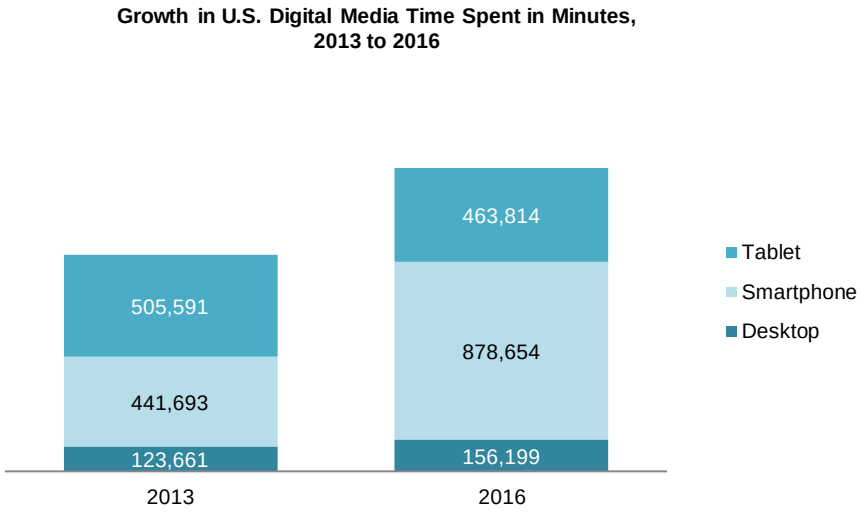
This is imperative from a fraud prevention perspective, but given all the compliance requirements related to AML and KYC, financial services firms must quickly and reliably confirm the identities of all applicants as well as verify identities of returning customers. As crime rings increasingly cultivate and monetize synthetic identities, it is increasingly difficult for businesses to balance KYC controls while still providing a positive customer onboarding experience.

GROWTH OF DIGITAL CHANNELS

Consumers are not only increasingly digital but are also increasingly mobile. Digital media usage has grown 40% since 2013, largely fueled by increased smartphone usage (Figure 1), with nearly one in eight U.S. consumers identifying themselves as mobile-only.

2. Peter Steiner cartoon, Condé Nast, accessed June 19, 2017, https://condenaststore.com/featured/on-the-internet-peter-steiner.html.

Figure 1: Digital Device Usage Rising, Driven By Mobile



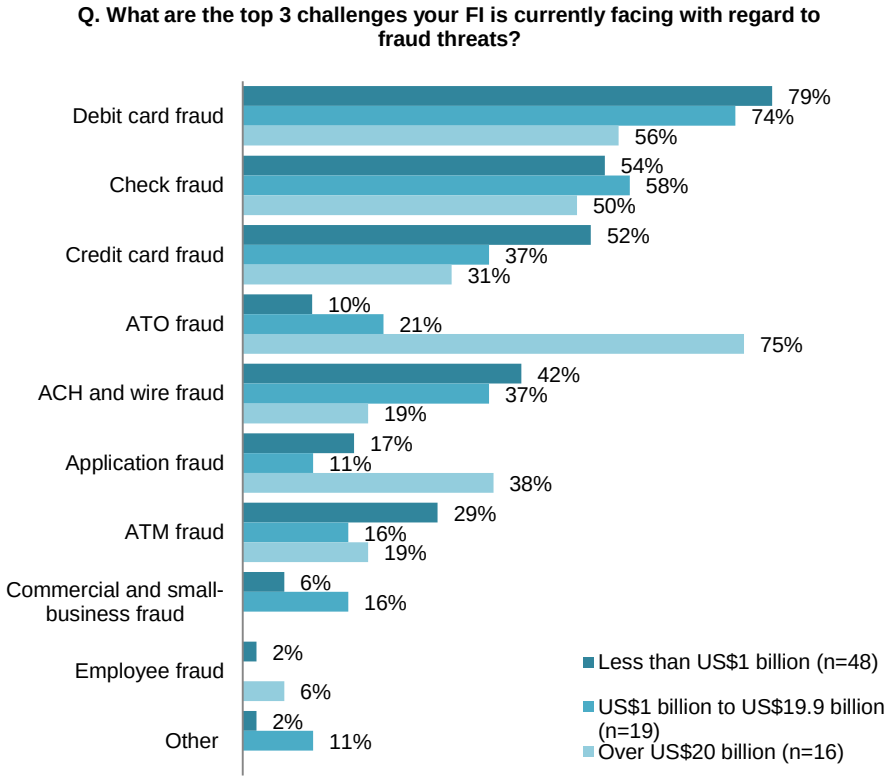
Source: comScore Mobile Metrix, 2017

Financial services firms want more customers to open new accounts, apply for loans, and transact digitally, because it is less expensive than manning physical branch locations or contact centers. Having consumer and provider preferences aligned is a happy coincidence except when the "customer" or "applicant" turns out to be a dog, i.e., a customer impersonator or fictitious identity.

APPLICATION FRAUD AND ATO

Application fraud rises in a post-EMV world, and the U.S. is no exception. Fraudsters must figure out how to replace the US$4 billion in counterfeit card fraud that will gradually disappear as EMV takes hold; two of the ways they will do so are through application fraud and through ATO. These trends were identified in other countries that rolled out EMV and were anticipated in the U.S., but they have not been prevented. Currently, in the United States, where EMV penetration is now over halfway complete, application fraud and ATO schemes are both hitting FIs very hard. A whopping 75% of FIs with assets over US$20 billion report that application fraud is one of their top three fraud challenges, and 38% of FIs of that size report that application fraud is one of their top three (Figure 2). While smaller percentages of FIs with assets under US$20 billion place these two types of fraud in their top three challenges, it is often the case that new fraud trends hit the largest FIs first, then as those FIs implement technology to protect themselves from the new threat, the attacks trickle down to smaller FIs. It is sometimes more difficult for smaller FIs to be able to afford new technologies to protect themselves, leaving them even more vulnerable to attack. An additional benefit of digital identity verification is that the cost can scale down to be affordable to FIs of all sizes.

Figure 2: Top FI Fraud Challenges by Asset Size



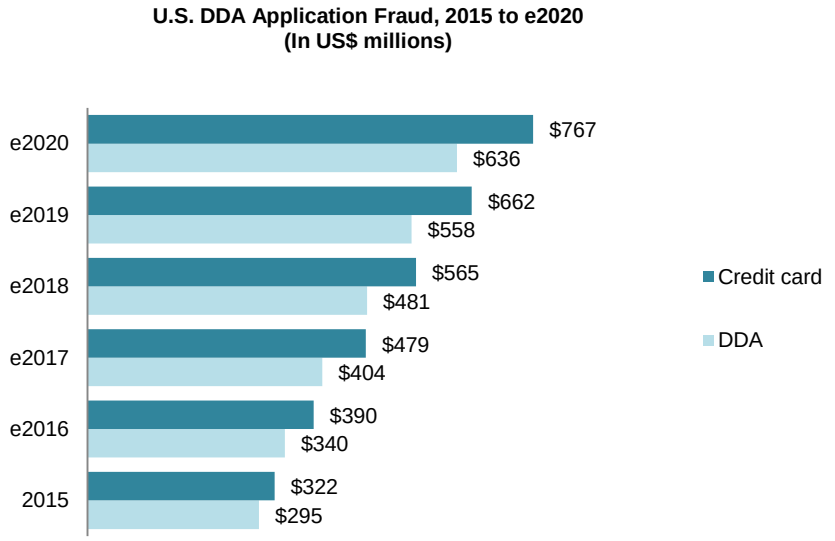
Source: Aite Group's survey of 83 U.S. FI executives, March and April 2017

These fraud attacks (and resultant losses) will continue to grow until FIs upgrade their identity verification solutions so that they can ensure they know the applicant applying for a new account or loan and they can appropriately identify existing customers accessing their accounts and funds. Both of these types of crimes are identity-related and can only occur in an environment in which identities are not vetted to the necessary degree.

Verifying identity documents can ensure the documents are valid. Comparing a selfie taken by a smartphone user can ensure that the person is the same individual pictured on identity documents and can perform a liveness test. This test is important to prove that the person actually is using the phone and not just submitting a photo stored on the device. This process can significantly reduce the threat of application fraud.

Figure 3 shows Aite Group's projection of the growth rate for application fraud in this post-EMV market for both credit cards and DDAs. As illustrated, fraudsters anticipated EMV rollout and began increasing such attacks prior to the implementation of EMV.

Figure 3: Projected Growth in Application Fraud



Source: Aite Group

Unfortunately, in the current environment, in which FIs are not able to consistently determine who they are dealing with in digital channels, fraud is not the only potential negative result; the FI may also have a serious compliance issue.

KNOW YOUR CUSTOMER

AML efforts are growing globally, with examiners in many countries raising their expectations of FIs' performance. In the U.S., the Bank Secrecy Act (BSA) defines the requirements for AML compliance. One of the foundational requirements of BSA mandates that FIs implement KYC processes. An argument could be made that all other compliance activities related to BSA are reliant upon effective KYC processes.

Few things instill fear in FI executives more than AML compliance violations. Not only can the FI be heavily fined, but there is also potential reputational damage as well as potential negative repercussions for individual employees. Recent trends indicate the compliance officer may particularly be vulnerable; repercussions can range from monetary fines to legal problems, including imprisonment.[3]

With a new applicant, how does an FI get to know its prospective customer? With the growing use of synthetic (or manufactured) identities,[4] it is increasingly difficult to determine that the applicant is who they claim to be.

All types of identity crimes are thriving in the digital world. The use of synthetic identities is growing rapidly; using these manufactured identities, fraudsters apply for loans or cards and never make the first payment. Similar fraud schemes occur with DDAs, which may be opened to commit fraud or to house funds stolen from other FIs. Another common fraud scheme involves customer impersonators who successfully convince contact center agents to reset online credentials, to place a check order, or to send an additional card on a credit account. All these methods of ATO occur without the legitimate customer being aware their account has been compromised. Using identity document verification before allowing changes to an account can quickly shut down the majority of these fraud attempts.

It is difficult to imagine how a compliance officer in an FI with major application fraud or ATO fraud losses can claim to have adequate, effective KYC procedures in place. While regulators haven't necessarily made this connection (due to their siloed approach to examinations), it seems inevitable that they eventually will do so.

OPERATIONAL EFFICIENCY IMPLICATIONS

FIs require that the applicants for new accounts provide some type of identity document to meet their KYC compliance requirements. Applicants may have to email or snail mail a copy of the identity document; if the documents are not received (after additional follow-up requests), the new account may have to be closed, or the FI may risk violating policy or regulatory requirements. Almost all of these processes require manual labor, further raising the cost of obtaining accurate customer data and identity documents for identity verification. Presenting

3. "Government enforcers take aim at compliance officers," Financial Times, May 2017, accessed June 26, 2017, https://www.ft.com/content/cc2a7072-3a62-11e7-821a-6027b8a20f23?mhq5j=e1.

4. See Aite Group's report *Financial Institution Fraud Trends: ATO and Application Fraud Rising Rapidly*, May 2017.

identity documents at the time of account application can save significant manual labor, improving operational efficiency in the process.

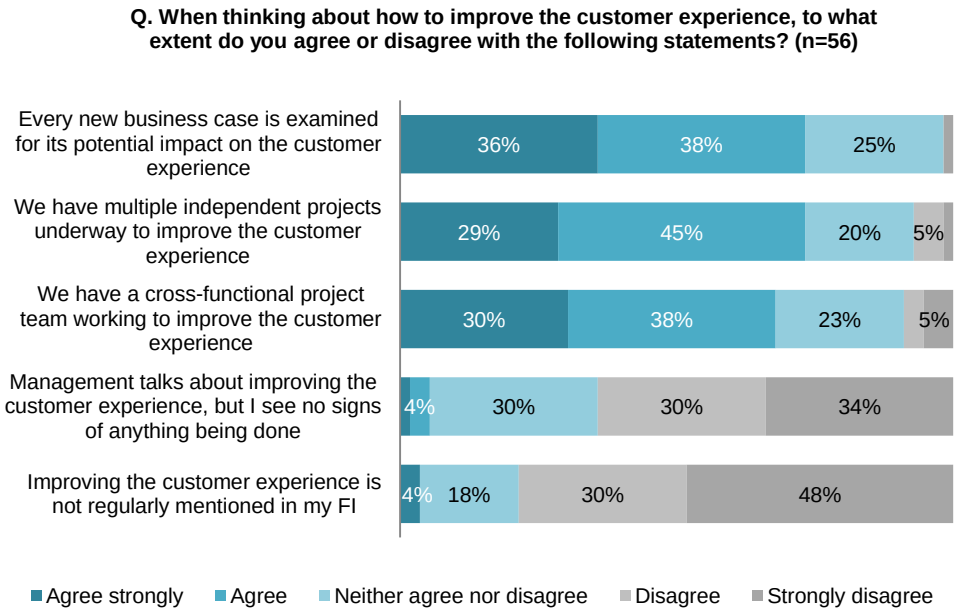
CUSTOMER EXPERIENCE

The expectation of consumers is that digital interactions should be easy, simple and convenient. This expectation applies to everything from applying for a new account to making a purchase or payment. While security is important to consumers, it is simply an expectation; consumers are not willing to be inconvenienced to improve security.

Financial services firms are hearing this requirement loud and clear, and they are taking many actions to improve the customer experience. Even fraud departments are being impacted, as every business case for a new fraud solution is examined for its impact on the customer experience. This makes sense, because even if a new solution is extremely effective, it cannot be successful if customer adoption is low. The most successful fraud and authentication solutions are easy for or transparent to the customer. Because consumers are using their mobile devices frequently for a wide variety of tasks, solutions utilizing those same devices may be welcomed by consumers. FI executives may label this as the "cool factor" in banking.

When consumers want to open a new account or apply for a loan online, offering a one-step solution without mandatory follow-up steps is efficient and customer-friendly. Minimizing keying requirements and ensuring that the identity of the consumer is verified can help prevent identity theft. Many financial services firms have a strong focus on improving the customer experience; the process improvements enabled by identity document verification can easily help meet the consumer's expectations of ease and convenience, resulting in a win-win situation (Figure 4).

Figure 4: Importance of the Customer Experience to FIs



Source: Aite Group's survey of 83 U.S. FI executives, March and April 2017

DOCUMENT AUTHENTICATION

Document authentication refers to verifying the authenticity of a document. Using document authentication can help financial services firms in many ways. Implementing the technology and building it into everyday procedures can yield the following benefits:

- Comply with AML regulations
    - Document authentication can assist with KYC compliance obligations. In the U.K., document authentication technology is a requirement for any digital-only bank to onboard a customer.
    - A number of countries in Europe have legislated that money services firms must digitally collect and store identity documents for cash transactions over a specific amount (e.g., Italy requires this for transactions over 1,000 euros); compliance is achieved with no additional steps.
- Improve the customer experience
    - Using the data on identity documents to prefill data on applications eliminates keying on small mobile keyboards, making the process faster and easier for the applicant.
    - Consumers like using their mobile devices, particularly if the process is fast and easy. In addition to speeding up the application process, the customer isn't inconvenienced by having to send in copies of identity documents later.
    - Collecting identity documents and verifying them during new account or loan application enables a financial services firm to determine whether they are dealing with a legitimate applicant, not a fraudster, so they can extend better offers or cross-sell other services with confidence.
    - In subsequent interactions, identity document verification may be used to re-authenticate customers and combat ATO fraud on existing accounts.
- Streamline operational processes, dramatically improving operational efficiency
    - Identity documents can be obtained and verified at the time of application, eliminating the need for follow-up identity screening.
    - Obtaining documents at the time of application eliminates costly follow-up processes to obtain copies of identity documents.
    - Using the information on identity documents to prefill application data fields eliminates keystrokes and makes the process easier.

Consumers want their digital interactions to be easy and convenient; if the benefits of using this method are explained, many consumers will readily engage.

MACHINE LEARNING

Verifying that a document is legitimate is an important first step in the process. Equally important is performing tests to ensure the data on the document hasn't been tampered with or changed in any way. Mitek performs many checks and tests on documents as part of the verification process. These tests include taking steps to ensure the data encoded on the document matches the data printed on the face of the document. In addition, Mitek knows what colors, fonts, security features, placement of various items (e.g., pictures), and other attributes are expected to appear on various documents, and it detects discrepancies on documents presented. Artificial intelligence and machine learning are used by Mitek to leverage and continually improve its ability to verify identity documents.

RECOMMENDATIONS

A perfect storm is forming for financial services firms as the digital threat environment continues to escalate, while an increasing proportion of transactional activity takes place in digital channels. The challenge for these firms is to effectively balance risk mitigation with a delightful customer experience. Here are a few recommendations that can help financial services firms achieve the optimal balance:

- Assess the current process for digital channel applications, determining current error rates, customer abandonment rates, etc.
- Determine whether a higher volume of applications and more accurate applications may be received with a more customer-friendly process.
- Assess the current cost of error correction and follow-up to obtain identity documents for KYC compliance.
- Assess the application fraud losses that are currently being incurred, understanding that some of those losses may be classified as credit losses (particularly loans that never received the first payment).
- Determine whether the use of some existing methods to achieve KYC compliance on new customers could be reduced or eliminated.
- Determine whether the need for some fraud screening may be eliminated with the use of document authentication.
- Calculate the benefits of approving more new accounts and loans via the mobile channel while adequately managing the risk from such applications.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Shirley Inscoe
+1.617.398.5050
sinscoe@aitegroup.com

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

ABOUT MITEK

Mitek uses artificial intelligence and machine learning, combined with document expertise, to provide fast and accurate digital identity verification. Financial services firms and organizations across industries use Mitek to achieve regulatory compliance and mitigate fraud risk for onboarding, money movement, and user authentication. Identity document verification helps financial services firms with the following:

- Comply with AML and KYC regulations
- Verify applicants from across the globe and collect reliable data on international documents
- Verify account holders during subsequent interactions with the financial services firm to combat ATO threats
- Mitigate fraud risk and reduce fraud losses
- Automate the identity verification component of new account opening, loan origination, and payment processes to improve operational efficiency and the digital customer experience

Mitek is headquartered in San Diego, California, with offices in London and Amsterdam, and it is publicly traded on Nasdaq (MITK). For more information, visit www.miteksystems.com.