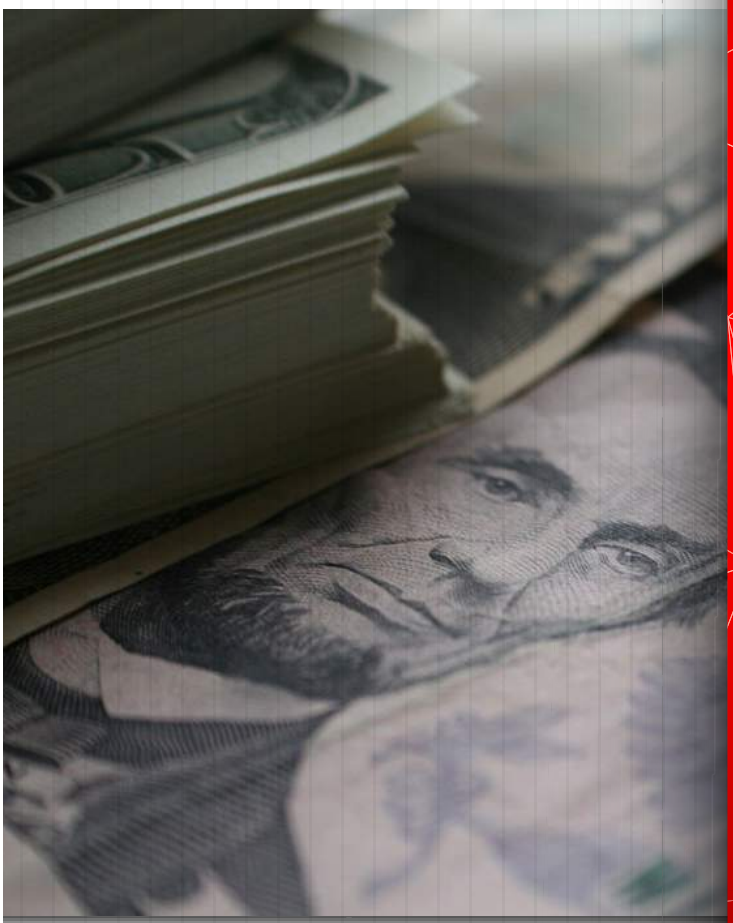
PYMNTS.com
what's next in payments and commerce

THE STATE OF ANTI MONEY LAUNDERING

MARCH 2017



2-4%

PERCENTAGE OF GLOBAL GROSS DOMESTIC PRODUCT (GDP) AT RISK OF BEING LAUNDERED[1]

<1%

PERCENTAGE OF MONEY-LAUNDERED FUNDS THAT ARE SEIZED AND FROZEN[2]

$14B

PENALTY THAT DEUTSCHE BANK MAY PAY IN FINE AFTER COMPLETION OF ITS ONGOING MONEY-LAUNDERING INVESTIGATION — THE HIGHEST FINE IN HISTORY[3]

$554M

DATA RECORDS STOLEN IN FIRST HALF 2016[4] — A 31 PERCENT INCREASE OVER THE PREVIOUS SIX MONTHS

70%

PERCENTAGE OF AMERICANS WHO OWN A SMARTPHONE. ALMOST 50 PERCENT OWN A TABLET[5]

79%

PERCENTAGE OF WORLD'S POPULATION THAT HAS OFFICIAL GOVERNMENT IDENTITY DOCUMENTATION[6]

Mitek

EXECUTIVE SUMMARY

Money laundering has a long and ancient history. From the age of gold coinage to today's technologically advanced banking system, it has continually evolved to survive and thrive in the changing times.

For years, it had predominantly been the fail-safe domain of drug cartels. Since 9/11, however, laundering money has become a lot harder than it used to be. In an effort to tighten the noose around terrorists using laundered funds to launch an attack, the American government has made each iteration of anti-money laundering (AML) legislation more complex: Standards are higher, and penalties for failure to comply are harsher. However, even today, many of the details remain vague, making it difficult for banks to effectively comply with AML rules.

Banks are also now responsible for "know your customer" (KYC) compliance and need to find technological solutions to do this, especially since several vulnerabilities still exist within the banking system.

In addition, as AML legislation has become more complex, fines for failure to comply have increased significantly. Between 2009 and 2015, the US government fined banks a total of $5.2 billion.

To avoid steep fines and remain compliant, banks are expected to know who is opening an account and the level of risk that each person presents. And in order to proactively combat fraudsters, banks have to invest in identity verification while still offering customers the seamless digital banking experience that they demand.

Mobile phones offer a variety of solutions for identifying customers and assessing their risk. Remote ID verification, combined with mobile devices offers an elegant solution for complying KYC regulations without inconveniencing customers.

Ultimately there are a variety of tools banks can use for identity verification on the market; however, not all of them are created equal. It is up to banks to determine which tools best serve their compliance needs without disrupting the lives of their customers. After all, with growth of terrorism, AML regulations will only continue to get stricter.

Cover Citations:

1 United Nations Office on Drugs and Crime. Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes. 2011. http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

2 United Nations Office on Drugs and Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes. 2011. http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

3 Coppola F. "Deutsche Bank: A Sinking Ship?" Forbes. September 27, 2016. http://www.forbes.com/sites/francescoppola/2016/09/27/deutsche-bank-a-sinking-ship/#5e5fb2c3b9bc.

4 Gemalto. Gemalto releases findings of first half 2016 Breach Level Index. September 20, 2016. http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-first-half-2016-Breach-Level-Index.aspx.

5 Statista. United States; Statista Market Analytics; 2010 to 2015; Individuals of any age who own at least one smartphone and use the smartphone(s) at least once per month. https://www.statista.com/statistics/201183/forecast-of-smartphone-penetration-in-the-us/.

6 The World Bank. Identification for Development. December 5, 2016. http://www.worldbank.org/en/programs/id4d.

The first records of money laundering date back to ancient China, when merchants hid their economic activities from the government since many forms of commercial trade were banned.[7] The term itself dates back to the 1920s during the American Prohibition, when gangsters such as Al Capone opened laundromats to mix the profits of their illegal business from selling alcohol with legitimate profits from laundry.[8]

Today, the proliferation of new and easy payment technologies means it's even easier for individuals to transfer sums of money across borders. A plethora of payment methods also means an excess of creative ways to transfer money illegally.

During the past 50 years, there's been a flurry of AML activity. Modern legal enforcement of money laundering in the United States started with the Bank Secrecy Act (BSA) of October 26, 1970.[9] The BSA initially required financial institutions (FIs) to help the American government prevent and detect money laundering. At first, one of the main focuses of AML laws was the War on Drugs. The BSA mandated FIs to keep a registry of customers' transactions and report transactions over a certain threshold as well as any suspicious transactions. These requirements meant that banks had to have a better knowledge of their clients, and the requirements became known as KYC procedures.[10]

However, after 9/11, AML programs shifted their focus to terrorists — who could wreak more havoc using fewer dollars — making it even more critical for banks and non-bank financial entities to understand who their customers are. The USA PATRIOT Act of 2001 expanded the scope of AML programs[11] and made regulations on suspicious activity reports, customer identification programs and customer due diligence (CDD) more stringent.

That was just the beginning of a worldwide movement to crack down on the illegal movement of money between parties. For example, the European Union (EU) enacted the fourth iteration of its Anti-Money Laundering Directive (the AMLD IV), which updated the EU regulations to be more in line with those of the U.S..[12] All EU member states must be compliant with the new mandates by June 26, 2017. The new regulation requires banks and FIs to assess each

7 Morris-Cotterill N. Money Laundering Risk Management and Compliance. http://www.countermoneylaundering.com/public/content/brief-history-money-laundering.

8 What Is Money Laundering? About Business Crime Solutions Inc. https://www.moneylaundering.ca/public/law/what_is_ML.php.

9 Public Law 91-507 (Oct. 26, 1970). U.S. Government Publishing Office. https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf.

10 Roth J, Greenburg D, Wille S. Monograph on Terrorist Financing, Staff Report to the Commission. National Commission on Terrorist Attacks Upon the United States. http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf.

11 U.S. Commodity Futures Trading Commission. Anti-Money Laundering. http://www.cftc.gov/IndustryOversight/AntiMoneyLaundering/index.htm.

12 PwC. "ML global alignment: Two steps forward, one step back. 2015. http://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/aml-global-alignment.pdf.

customer's risk profile, shifting the burden of compliance on FIs to be proactive about identifying risky customer behavior.

Given the rapidly evolving pace of digital payments, this is likely only a harbinger of things to come. FIs can expect regulators to clamp down further as governments are forced to cope with the creative ways in which new technologies can be used and abused. FIs in the U.S. will be no exception, given the gaps now present in the existing regulations.[13] For example, a December 2015 study by LexisNexis found that while most banks already ask for the identity of account owners, only half verify their actual identity.[14]

PYMNTS, in conjunction with Mitek, has produced this special report, which examines the evolution of money laundering, the state of play in the regulatory arena, and how these existing vulnerabilities and application of new technologies may influence the actions of innovators to help ensure compliance.

13 Financial Action Task Force. Anti-money laundering and counter-terrorist financing measures - United States. 2016. http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

14 Rubenfeld S. Critics Find Flaws in U.S. Financial Transparency Rule. The Wall Street Journal. May 9, 2016. http://blogs.wsj.com/riskandcompliance/2016/05/09/critics-find-flaws-in-u-s-financial-transparency-rule/.

VULNERABILITIES WITHIN THE BANKING SYSTEM

Estimating the amount of money that is laundered globally is difficult. The last estimate was done by the United Nations (UN) in 2011, updating 1998 statistics. According to the UN, between 2.1 and 4 percent of the GDP is at risk of being laundered, roughly the same statistics from 1998. However, less than 1 percent of these funds are seized and frozen.[15]

The U.S. Treasury Department has identified the following money laundering vulnerabilities in the U.S.' banking sector[16]:

- **Structuring:** Structuring involves dividing large transactions into several smaller ones to avoid the BSA's threshold. Some of these techniques are used by Mexican drug cartels to funnel drug proceeds to the Southwest border region as a first step for smuggling cash into Mexico.
- **Misuse of correspondent banking services:** Frequently, when transactions cross international borders, banks keep limited records, which means some accounts and transactions can fly under the radar and be used to launder money.
- **Misusing prepaid debit cards:** These cards can function as an alternative to cash. They can easily be purchased and then cashed, similar to money orders and travelers' checks.
- **Nominees and misuse of legal entities:** This refers to using a bank account under someone else's name or a business' name to transfer or keep illegal funds. However, this can be prevented using basic and advanced KYC methods.
- **Money brokers:** In April 2006, the U.S. Treasury alerted financial institutions that U.S. currency smuggled into Mexico often made its way back into the U.S. through U.S. correspondent accounts held by Mexican banks and currency exchangers.
- **Trade-based money laundering:** Restrictions on money brokers led some cartels to mix their legal and illegal businesses in order to disguise the origin of their illegal income.
- **Misuse of third-party payment processors:** Since 2005, the U.S. Treasury has issued warnings about unscrupulous third-party payment processors, which have been associated with not only money laundering, but also identity theft and fraud.

However, these are just the vulnerabilities in the banking sector. Other sectors such as money services, casinos and securities markets all have their own vulnerabilities, which are frequently exploited. It is very likely that the U.S. will be drafting more regulation in the future to address these gaps.

15 United Nations Office on Drugs and Crime. Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes. 2011. http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

16 Department of the Treasury. National Money Laundering Risk Assessment 2015. Washington, D.C. https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

Fines for non-compliant banks have been increasing significantly — and in all probability fines will continue to increase in the future as AML restrictions tighten. According to the U.S. GAO, the U.S. government fined banks $5.2 billion in total between 2009 and 2015.[17] Between 2016 and January 2017, more than $15 billion in fines were announced.

Failure to comply with AML regulations has not only affected banks, but also other institutions. In the gambling businesses, for instance, some of the most notable failures were: Caesars Entertainment Corp., which was fined $9.5 million for deficient AML controls[18], Trump Taj Mahal casino, which was fined $10 million for violating the BSA "program reporting and record-keeping requirements,"[19] and the Tinian Dynasty Hotel & Casino that was fined $75 million by the FinCEN.[20]

Table 1 summarizes some of the most notable fines over the past few years.

The total amount fined since 2009 represents just a fraction of money that has been laundered over the years. However, with tightening regulations, the list of institutions being fined is now quickly starting to grow longer.

Table 1. Important AML Fines since 2009

Case	Year	Fine	Description
Wachovia Bank	2010	$160M	Internal controls failed, enabling drug traffickers to launder money
Royal Bank of Scotland	2010	$100M	Failed to disclose identity information of sanctioned parties for 3,500 transactions valued at $523 million
HSBC Bank	2012	$1.92B	Set up offshore accounts for drug cartels and suspected criminals in New Jersey between 2003 and 2010
MoneyGram	2012	$100M	Aided and abetted criminal wire fraud and failed to maintain an effective AML program
JP Morgan	2014	$2B	Failed to report suspicious Bernie Madoff investments
Commerzbank	2015	$1.45B	Did business with Iran and other sanctioned countries and failed to implement adequate AML controls
Deutsche Bank	2015	$258M	Cleared $10.9 billion transactions between 1999 and 2006 using "non-transparent methods and practices"
Tinian Dynasty Hotel & Casino	2015	$75M	The casino operated for years without an AML program. It failed to file thousands of CTRs and its management willfully facilitated suspicious transactions and even provided helpful hints for skirting and avoiding the laws in the U.S. and overseas.
Deutsche Bank[21]	2016	$14B	Allegedly mis-sold bonds prior to the 2008 financial crisis
Agricultural Bank of China	2016	$215M	Obscured clearing dubious transactions, including counterfeiting and falsifying invoices and omitting information regarding possible U.S. dollar trades
Mega International Bank	2016	$180M	Inconsistent transaction monitoring policies and procedures, failed to properly conduct CDD and had inadequate risk assessment policies and procedures
Western Union	2017	$586M	Turned a blind eye on criminals using its services to commit money laundering and fraud

AML, anti-money laundering; CDD, customer due diligence; SAR, Suspicious Activity Report.

17 Government Accountability Office. Financial Institutions: Fines, Penalties and Forfeitures for Violations of Financial Crimes and Sanctions Requirements. 2016. http://gao.gov/assets/680/675987.pdf.

18 O'Keeffe K. Caesars Fined $9.5 Million Over Lax Money-Laundering Controls. The Wall Street Journal. September 8, 2015. https://www.wsj.com/articles/u-s-fines-caesars-8-million-over-money-laundering-controls-1441721034.

19 Brickley P. Trump Taj Mahal Settles Over Anti-Money-Laundering Violations. The Wall Street Journal. February 11, 2015. https://www.wsj.com/articles/trump-taj-mahal-settles-over-anti-money-laundering-violations-1423669834.

20 Hudak S. FinCEN Fines Tinian Dynasty Hotel & Casino $75 Million for Egregious Anti-Money Laundering Violations. FinCEN. June 3, 2015. https://www.fincen.gov/news/news-releases/fincen-fines-tinian-dynasty-hotel-casino-75-million-egregious-anti-money.

21 This is still an ongoing case, and the penalty has not been levied yet.

Some other regulated institutions fined during this period include the following:

Case	Year	Fine
Pamrapo Savings	2010	$1M
Ocean Bank	2011	$11M
AAA Cash Advance	2012	$2.25M
Oppenheimer & Co.	2015	$20M
CommerceWest Bank	2015	$4.9M
Bank of Mingo	2015	$4.5M
Caesars Entertainment Corp	2015	$9.5M
Trump Taj Mahal	2015	$10M
Credit Suisse Securities	2016	$16.5M
Standard Chartered Bank	2016	$5.5M
Florida Gibraltar Bank	2016	$4M
Hawaiian Gardens Casino	2016	$2.8M
Swedbank AS	2016	$1.53M
Gala Coral	2016	£850,000
Banco Santander	2016	$1.1M
Paddy Power	2016	$400,000

KYC requirements for AML compliance

So what does it take not to get fined? KYC is the key to compliance. The Financial Action Task Force, an intergovernmental body, recommends that KYC and CDD measures should include the following[22]:

- Identifying the customer and verifying customer identity
- Identifying the account owner
- Understanding and obtaining information on the purpose and intended nature of the business relationship
- Ensuring through ongoing analysis that transactions are "consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds"
- Other pieces of the KYC process involve background checks for criminal records, political exposure and country of citizenship. The extent of these measures should depend on the amount of risk each customer or business transaction presents.

However, there's no standard for implementing KYC, nor are there mandated technologies to ensure KYC is carried out. Meanwhile, KYC guidelines are vague but accompanied by harsh fines for failure to comply. Banks have a strong incentive to comply, but what they should do is unclear, and there are a variety of options to choose from.

22 de Koker L. Anonymous Clients, Identified Clients and the Shades in Between – Perspectives on the FATF AML/CFT Standards and Mobile Banking. SSRN. September 4, 2009. https://ssrn.com/abstract=2634305 and http://dx.doi.org/10.2139/ssrn.2634305.

The most traditional form of KYC is having a customer go to a bank to get their personal identification documents verified. However, that's just the first step, and in this day and age of internet banking, KYC technologies cover several different bases behind the scenes, including:

- **Knowledge-based authentication (KBA):** Users must answer personal questions as they log into their accounts, making it much more difficult for fraudsters to crack accounts. However, in many cases, it's not difficult for fraudsters to find KBA publicly listed, such as birthdates or college alma maters.
- **Sanctions check tools:** These compare potential customer lists to government lists of politically exposed persons, as well as people with criminal track records.
- **Credit data:** These tools analyze a customer's credit data and calculate the amount of risk they represent.
- **Analytics solutions:** These Big Data solutions, whether provided by an external vendor or internally engineered, can analyze customer transaction data and flag unusual behavior patterns such as transactions coming from or going to an atypical location. However, these tools are not perfect and can often make customers' lives more difficult. For example, if a customer is traveling and doesn't notify their FI, their transaction might be declined because it's "fraudulent."

- **Data bureaus:** These are solutions that involve collaboration between several institutions that share information about their customers. Therefore, they work as a tool to enlarge databases and gather information about company customers.

GETTING STRICTER —
AND WILL THEY CONTINUE TO DO SO?

AML originally started as part of the War on Drugs. However, after 9/11, AML shifted its purpose to focus on preventing terrorism, where the stakes were much higher. While drug cartels were primarily focused on making money, with violence occurring as a side product, the direct aim of terrorism was to, well, terrorize. Terrorists reverse money laundering. Drug cartels try to make illegally obtained money look legal so they can spend it; terrorists try to take legal funds and spend them on illegal activities. Terrorists, without doubt, are capable of wrecking havoc with fewer resources. Between 2006 and 2013, terrorism resulted in 130,000 deaths.[23] By 2014, there were nine times the number of terrorist attacks that there were in 2000,[24] and in 2016, terrorist attacks were a near daily occurrence across the globe.[25] Strict AML regulation is no longer just about money laundering — it's also about maintaining the safety of society.

Europe's recent update to their AML resulted in significantly stricter regulations, which mirror America's AML programs, which were expanded after 9/11. The new AML regulations (which place a higher burden on banks) focus on ensuring that banks know exactly who is opening and accessing accounts, and can calculate the level of risk they present. While the regulations don't provide much in the way of guidance, they do come with heavy fines, implying a "no excuses" approach.

Despite existing KYC technologies in place, banks are still vulnerable. As exemplified in Table 1 earlier in this report, several of the banks listed, such as Mega Bank, had AML procedures in place, yet these procedures failed them. In fact, banks are projected to spend $8 billion on AML in 2017, and an American Bankers Association survey found that 46 percent of small banks said they had to reduce their products and services because of compliance costs.[26] Banks are clearly trying, but what they are doing isn't working.

Given the number of banks that have been slapped with fines under existing AML regulations, it is doubtful AML is going away anytime soon.

23 Statista. Facts and statistics on terrorism. https://www.statista.com/topics/2267/terrorism/.

24 Costa Roberts D. 4 surprising facts from the 2015 Global Terrorism Index. PBS. November 23, 2015. http://www.pbs.org/newshour/rundown/4-surprising-facts-from-the-2015-global-terrorism-index/.

25 Dorrell O. 2016 already marred by nearly daily terror attacks. USA Today. June 29, 2016. http://www.usatoday.com/story/news/world/2016/06/29/major-terrorist-attacks-year/86492692/.

26 Pelaez C. AML Compliance Costs — How Much Is Enough? GlobalRadar.com. https://www.globalradar.com/aml-compliance-costs-how-much-is-enough/.

MOBILE PHONES TO THE RESCUE!

However, mobile phones present a plethora of exciting possibilities for verification and assessing customer risk. These include:

- **Geolocation and carrier network data:** This can be used to figure out where a phone is located and what service a phone uses, which is useful for identifying risk level but provides very little in the way of actually verifying the owner's identity.
- **Biometric data:** Biometric authentication detects a physical characteristic of the phone user, such as voice, digital prints or facial characteristics, and compares them with characteristics stored in a database. However, implementing this requires a lot of effort on the part of FIs to build this database.
    - **Keystroke biometrics:** These recognize a user by their cellphone based on the typing patterns. While this method adds an extra layer of security, it is not entirely reliable as typing patterns can change (for example, if a person undergoes physical trauma or injury).
    - **Mobile ID document verification:** This entails using mobile phones to allow bank users to authenticate and verify physical identity documents, such as government-issued IDs. It leverages the technology that is now in place for banks to enable mobile remote check deposit, giving banks a tool and technology platform that serves a dual purpose.

As AML regulation amps up even further, savvy FIs will increase their KYC technology accordingly. Institutions that use dated technologies are making themselves vulnerable to attack. Not only do they risk heavy fines, they also risk having their customer data stolen and losing millions of dollars, as was the case with the Bangladesh Central Bank, Tesco Bank, Ecuador's Banco del Austro or JP Morgan & Chase in their 2014 data breach.

The combination of smartphones and government-issued identities creates a powerful and credible weapon for FIs to fight against money laundering: mobile image capture of identity documents.

Smartphones and government-issued IDs are ubiquitous. Nearly 70 percent of people in the U.S. have a smartphone, and almost 50 percent own a tablet.[27] An estimated 79 percent of the world's population has official government documentation.[28] A growing number of developing countries are creating programs to ensure all citizens have an ID, and the World Bank is working with those countries to close this gap by 2030, with its new Identification for Development Initiative.

Mobile image capture of identity documents uses algorithms that can confirm if a document is a legitimate government-issued document. Once the image passes a certain quality-level threshold, algorithms can recognize and classify government IDs from around the world. After the image has been sorted into categories, the ID verification technology can extract the relevant data to analyze the ID's contents to ensure that it is a real government-issued document. Mobile capture-based identity verification can go even a step further. After the ID document has been verified, the user can prove that they are, in fact, the person represented by the ID by taking a selfie that is compared against the ID photo.

This process uses a facial comparison to verify that the customer is actually a real person and then matches the selfie picture against the photo on the ID documents. The algorithms need to take into account potentially challenging ID photo quality and that the ID holder's appearance may have changed since the ID photo was taken. All of this can be done without the customer leaving their home.

The new AML regulation supports the use of technological solutions, noting that "accurate identification and verification of data of natural and legal persons is essential for fighting money laundering or terrorist financing. Latest technical developments in the digitalization of transactions and payments enable a secure remote or electronic identification."[29]

Leveraging these solutions to verify IDs is the clearest solution for FIs that wish to be proactive about AML regulations. In all likelihood, regulations for AML initiatives will only continue to become more stringent. Mobile capture-based identity proofing of identity documents and its owners allows FIs to screen out potential threats while still offering customers the seamless experience they have come to expect and value.

27 Statista. United States; Statista Market Analytics; 2010 to 2015; Individuals of any age who own at least one smartphone and use the smartphone(s) at least once per month. https://www.statista.com/statistics/201183/forecast-of-smartphone-penetration-in-the-us/.

28 The World Bank, Identification for Development. December 5, 2016. http://www.worldbank.org/en/programs/id4d.

29 Clark S. "Leveraging Digital Identity Verification to Stay on Top of New AML Regulations." Finextra. September 15, 2016. https://www.finextra.com/blogposting/13095/leveraging-digital-identity-verification-to-stay-on-top-of-new-aml-regulations.

ABOUT

About Mitek

Mitek (NASDAQ: MITK) is a global leader in mobile capture and identity verification software solutions. Mitek's ID document verification allows an enterprise to verify a user's identity during a mobile transaction, enabling financial institutions, payments companies and other businesses operating in highly regulated markets to transact business safely while increasing revenue from the mobile channel. Mitek also reduces the friction in the mobile users experience with advanced data prefill. These innovative mobile solutions are embedded into the apps of more than 5,400 organizations and used by tens of millions of consumers daily for new account openings, insurance quoting, mobile check deposit and more. For more information, visit www.miteksystems.com.

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

DISCLAIMER

The State of Anti Money Laundering Report™ may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

You agree to indemnify and hold harmless, PYMNTS.COM, its parents, affiliated and related companies, contractors and sponsors, and each of its respective directors, officers, members, employees, agents, content component providers, licensors, and advisers, from and against any and all claims, actions, demands, liabilities, costs, and expenses, including, without limitation, reasonable attorneys' fees, resulting from your breach of any provision of this Agreement, your access to or use of the content provided to you, the PYMNTS.COM services, or any third party's rights, including, but not limited to, copyright, patent, other proprietary rights, and defamation law. You agree to cooperate fully with PYMNTS.COM in developing and asserting any available defenses in connection with a claim subject to indemnification by you under this Agreement.