Aite PARTNER. ADVISOR. CATALYST.

Identity Verification: Successful Strategies to Minimize False Positives and Risk

JANUARY 2019

Prepared for:

melissa®

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
INTRODUCTION 4
METHODOLOGY 4
IDENTITY VERIFICATION CHALLENGES 6
THE FALSE POSITIVE CHALLENGE 8
THE NEED FOR NEW SOLUTIONS 10
MELISSA: REDUCING IDENTITY VERIFICATION HEADACHES 12
MOBILE PHONE VERIFICATION 13
CONCLUSION 14
ABOUT AITE GROUP 15
AUTHOR INFORMATION 15
CONTACT 15
ABOUT MELISSA 16
CONTACT 16

LIST OF FIGURES

FIGURE 1: ASSET SIZE OF FI RESPONDENTS 4
FIGURE 2: IMPACT OF DATA BREACHES ON FRAUD RATES 6
FIGURE 3: U.S. APPLICATION FRAUD LOSSES THROUGH 2020 7
FIGURE 4: FACTORS DRIVING INVESTMENTS 8
FIGURE 5: MANUAL REVIEW RATES 9
FIGURE 6: PLANNED CHANGES IN DDA APPLICATION RISK ASSESSMENT VENDORS 10
FIGURE 7: STRATEGIC IMPORTANCE OF INVESTMENT IN ANTI-FRAUD TECHNOLOGY 11
FIGURE 8: MELISSA RETURNS MATCH INFORMATION ON MANY ATTRIBUTES 12

EXECUTIVE SUMMARY

Identity Verification: Successful Strategies to Minimize False Positives and Risk, commissioned by Melissa and produced by Aite Group, discusses the challenges associated with new-customer identity verification that accomplishes bankers' goals of effective fraud prevention and Know Your Customer (KYC) compliance while minimizing friction in the customer experience.

Key takeaways from the study include the following:

- Application fraud will cause more than US$2.7 billion in U.S. credit card and demand deposit account (DDA) fraud losses through 2020.
- At the same time that the threat environment is sharply escalating, the pressure to reduce or even eliminate friction from the customer experience is also growing. When asked about key business case drivers for new-account risk assessment tools, 88% of the fraud executives surveyed indicate that improving the customer onboarding experience is a key business case driver.
- As a result of the escalating threat environment, combined with the competitive pressure to reduce friction, nearly half of respondents plan to either change or add new-account risk assessment vendors in the next couple years. This is an increase from 2015, when only 27% of survey respondents planned to add or change new-account risk assessment vendors.
- Melissa's global database supports both deterministic and probabilistic matching strategies to optimize matching routines. Melissa also applies advanced link analysis and entity resolution, not only to its own data, but also to its customers' data to minimize duplicate matches.
- Effective fraud prevention is increasingly a competitive issue for financial services firms. Early adopters of next-generation technologies will be able to do more than reduce fraud; the associated improvements to the customer experience give them a decided advantage over their competitors that lag in these investments. Data is the new currency, and creating intelligence from data at scale can give firms a competitive edge.

INTRODUCTION

Time is money when it comes to financial crime mitigation. Organized crime rings, fueled with billions of compromised data records, are systematically and methodically targeting financial services firms with sophisticated application fraud attacks that use stolen or falsified identities in an effort to obtain new accounts. The trajectory of these attacks continues to increase, since there is very little in the way of adverse consequences (i.e., jail time).

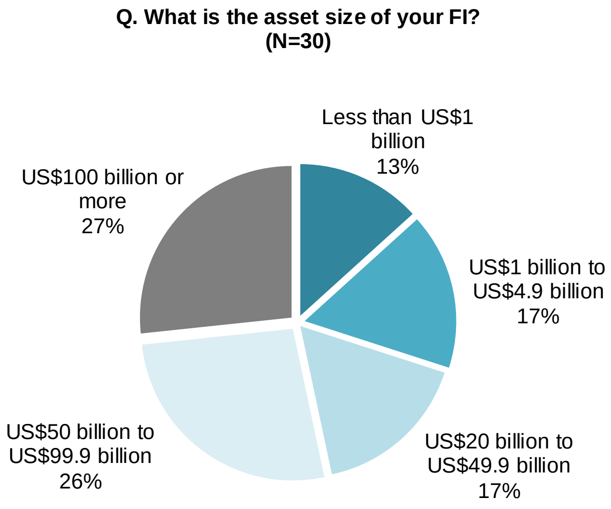
A key challenge for fraud and anti-money laundering (AML) executives is that even as the threat environment continues to escalate, financial institutions (FIs) are under intense competitive pressure to make the banking experience easy and frictionless. In the face of this seemingly contradictory set of mandates, many FIs are looking for better solutions to help with identity verification at onboarding.

This white paper discusses the challenge of verifying identity without intruding on the customer experience, and the operational impact of false positives. It addresses the need for next-generation solutions to help with identity verification and presents Melissa's approach to addressing these problems.

METHODOLOGY

Aite Group surveyed executives from U.S. FIs from March 2018 to June 2018 to better understand application fraud trends for both DDAs and credit cards. Asset sizes of participating FIs range from under US$1 billion to over US$100 billion (Figure 1). The survey was a refresh of a similar survey conducted in 2015—comparisons between the two data sets are made within the white paper.

Figure 1: Asset Size of FI Respondents



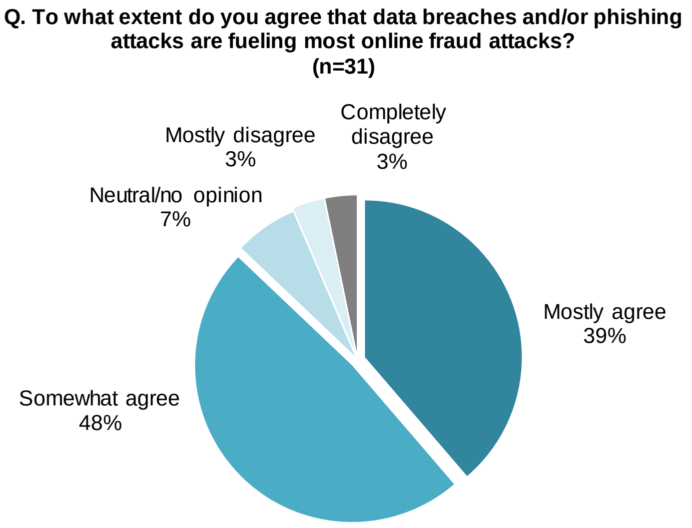
Source: Aite Group's survey of 30 FIs, March to June 2018

The white paper is also informed by an Aite Group survey of 32 U.S. financial crime executives in September 2018 about pain points and planned technology spend. All bank respondents to the September 2018 survey come from larger institutions with more than US$30 billion in assets. Given the size and structure of the research samples, the data provide a directional indication of conditions in the market.

IDENTITY VERIFICATION CHALLENGES

With over 13 billion data records stolen or lost since 2013, organized crime rings have plenty of fodder to fuel their attacks on the financial services ecosystem.[1] The impact of the data breaches is significant. Eighty-seven percent of financial crime executives surveyed by Aite Group believe that data breaches or phishing attacks are responsible for the bulk of digital channel fraud (Figure 2).

Figure 2: Impact of Data Breaches on Fraud Rates

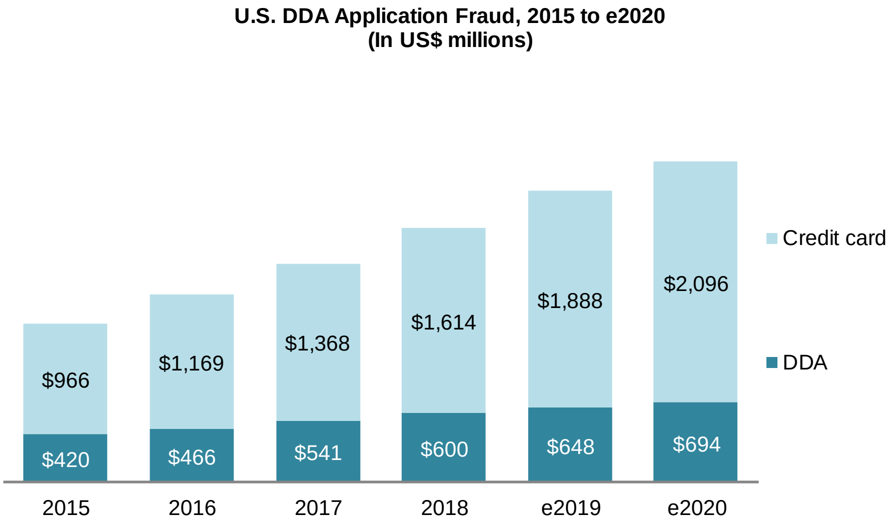


Source: Aite Group's survey of 32 financial crime executives, September 2018

Application fraud manifests as identity theft (the attacker is using the full identity of the victim) or synthetic identity fraud (fraudsters either create a new identity from scratch or compile bits and pieces of stolen data to establish a new identity). The combined impact of these attack vectors will cause more than US$2.7 billion in U.S. credit card and DDA fraud losses through 2020 (Figure 3).

[1] "Breach Level Index," accessed on December 7, 2017, http://breachlevelindex.com.

Figure 3: U.S. Application Fraud Losses Through 2020

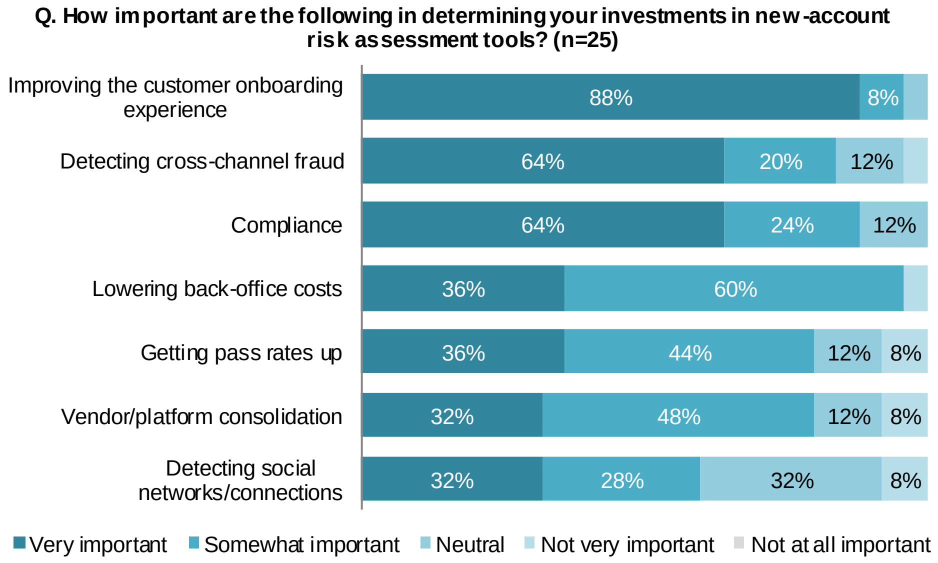


Source: Aite Group

At the same time that the threat environment is sharply escalating, the pressure to reduce or even eliminate friction from the customer experience is also growing. Consumers' expectations are increasingly shaped by the experiences provided by Apple, Lyft, and Amazon. FIs are under pressure to provide similarly friction-free and elegant interactions. The importance of ease of use starts at onboarding—FIs still see high levels of attrition with digital channel onboarding when hurdles in the process trip up prospective customers.

The importance of customer experience is borne out by the data in Figure 4. When asked about key business case drivers for new-account risk assessment tools, 88% of the fraud executives surveyed indicate that improving the customer onboarding experience is a key business case driver. While fraud detection and KYC compliance are also very important for 64% of respondents, customer experience obviously carries more weight for the majority of those surveyed.

Figure 4: Factors Driving Investments



Source: Aite Group's survey of 30 FIs, March to June 2018

THE FALSE POSITIVE CHALLENGE

Identity verification is an essential element of onboarding new banking customers. It is mandated by KYC regulations in countries around the globe and is a requisite element of FIs' fraud prevention needs. Identity verification is by no means a straightforward task, however, and when it comes to removing friction from the onboarding experience, reducing the false positives associated with identity verification is a key area of opportunity.

In the U.S., there is no primary data source available to query an individual's identity. Instead, businesses query data repositories that are compiled based on a variety of public data sources (e.g., U.S. Postal Service data) as well as repositories established by reported trade lines (e.g., credit bureau data). Leveraging these secondary data sources for identity verification comes with a variety of challenges:

- Businesses that report to the repositories often do not submit perfect data—there are mistakes such as fat-finger errors, old addresses, and even name changes.
- Customers and front-line staff are often guilty of their own fat-finger errors, meaning that often a mistyped application is being matched against mistyped public record data.
- While fuzzy matching can help with fat-finger issues and identifying fraudsters' intentional efforts to manipulate identities, it often leads to high rates of alerts that must be manually reviewed.

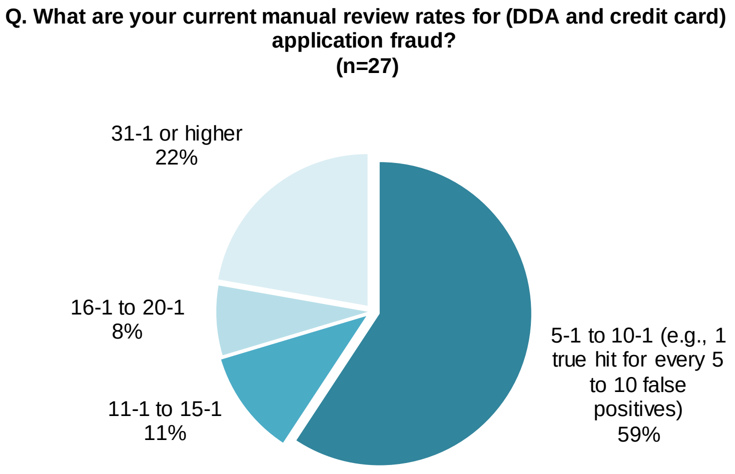
Identity matching is particularly problematic with data fields such as address; for example, some addresses contain multiple words (which may not always be included), and abbreviations that don't match can also cause false positives. At times, every dweller in an apartment complex may be triggered due to a fuzzy logic address match, causing an explosion in manual review. Another example involves names; a consumer may officially be a “Junior” but may not always use that suffix as part of his name, or he may abbreviate it to “Jr.” Such abbreviations can also be problematic in name matching, resulting in additional manual review volume.

Fat-finger errors not only increase manual review rates but are also expensive. In many cases, the errors require contact with the applicant to ensure the data is corrected appropriately, and the corrected data then has to be passed through all the fraud filters again. Rerunning credit bureau queries and other fraud filters results in additional charges from those vendors.

Human staff is always the largest expense line item for an FI, so any processes that require increased human effort are costly. The higher manpower requirement to address high false positive rates just increases the expense of fraud prevention; the only alternative (which some FIs embrace out of necessity) is to decision as many alerts as possible and delete the rest. Needless to say, unless alerts are prioritized well in terms of risk, fraudulent items can be missed with this approach.

Manual review rates tend to be high for application fraud due to the challenges of effective identity verification. Twenty-two percent of respondents report manual review rates at 31-to-1 or higher (meaning only one true hit for every 31 or more false positives,) while 41% of respondents report false positive rates greater than 11-to-1 (Figure 5).

Figure 5: Manual Review Rates



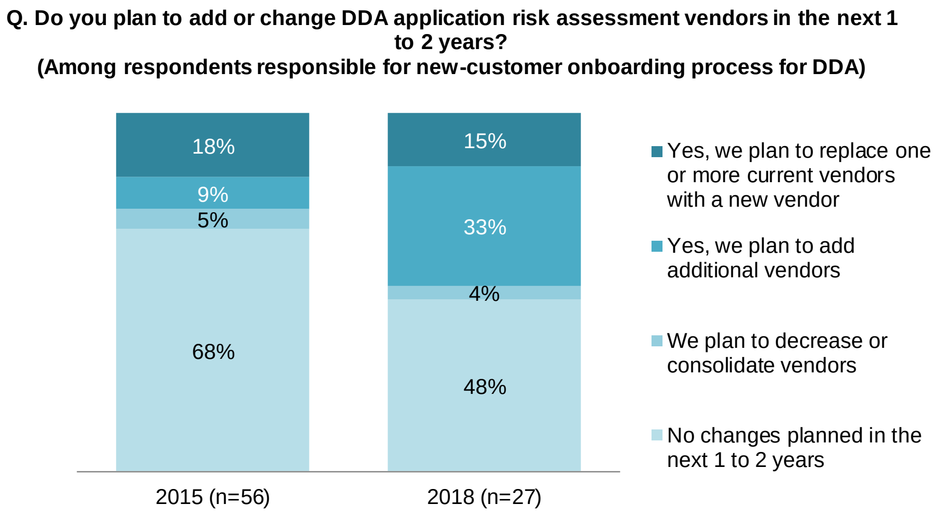
Source: Aite Group’s survey of 30 FIs, March to June 2018

These high rates of manual review are particularly problematic as financial crime executives are under intense pressure from their management and investors to reduce operational expenses(OpEx)—the ongoing expectation for most of the FI executives interviewed is OpEx reductions of 10% or more. Conversely, if FIs can become more efficient by reducing current manual review rates, they can shift existing resources to new types of fraud queues, such as real-time payments, without adding staff.

THE NEED FOR NEW SOLUTIONS

As a result of the escalating threat environment, combined with the competitive pressure to reduce friction, nearly half of respondents plan to either change or add new-account risk assessment vendors in the next couple of years. This is an increase from 2015, when only 27% of respondents planned to add or change new-account risk assessment vendors (Figure 6).

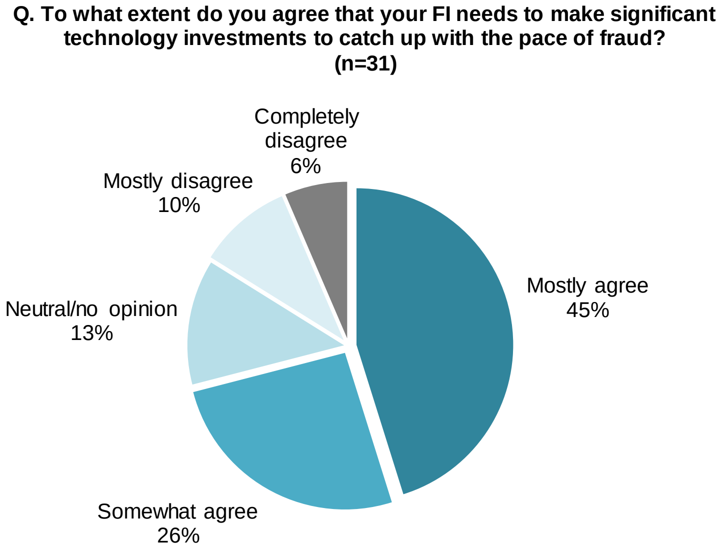
Figure 6: Planned Changes in DDA Application Risk Assessment Vendors



Source: Aite Group’s survey of 30 FIs, March to June 2018, and Aite Group’s survey of 83 U.S. FIs, November to December 2015

The importance of ongoing investment in new technology cannot be understated. Seventy-one percent of financial crime executives from larger firms believe that their financial services firm needs to make substantial investments to catch up with the pace of fraud (Figure 7).

Figure 7: Strategic Importance of Investment in Anti-Fraud Technology



Source: Aite Group's survey of 32 financial crime executives, September 2018

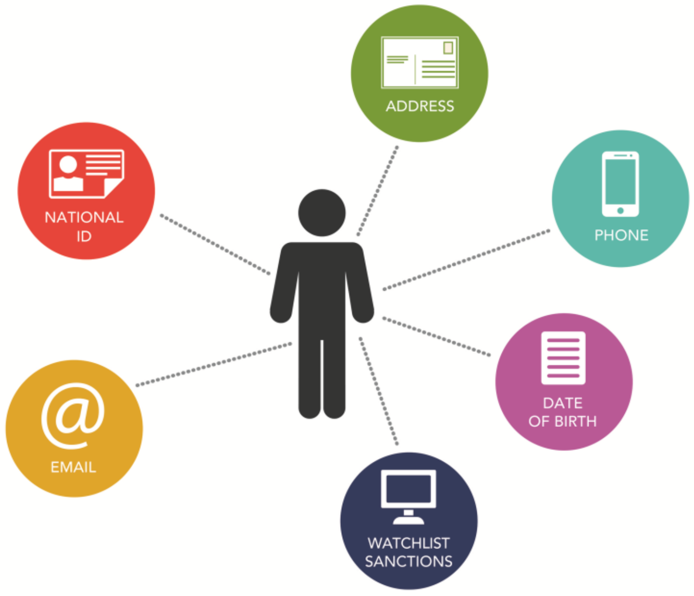
The pace with which fraud is escalating and accelerating is not the only issue. Effective fraud prevention is increasingly a competitive issue for financial services firms. Those that are early adopters of next generation technologies will be able to do more than reduce fraud; the associated improvements to the customer experience give them a decided advantage over their competitors that lag with these investments. Data is the new currency, and creating intelligence from data at scale can give firms a competitive edge.

MELISSA: REDUCING IDENTITY VERIFICATION HEADACHES

As FIs look for new ways to address the dual challenges of reducing customer friction and mitigating fraud risk, Melissa provides a solution. Melissa's ID Verification technology uses a multilayered process to access authoritative in-country data sets from all over the world containing billions of records to instantly validate an identity. The proofing process also includes national ID and age verification, and flags suspicious individuals who appear on any of dozens of Office of Foreign Assets Control and European Union watchlists to minimize risk and enable smarter decisions on what to do next: approve, deny, or escalate.

Melissa's long history of normalizing data according to established standards has resulted in specialized domain knowledge that increases match accuracy and reduces false positives, while ensuring the incoming data is valid in the real world and corroborates the customer's identity. When data quality is not part of the onboarding solution, the match technique between incoming identities and the repository rely on the simplest form of exact matching. Without data quality, inferior identity verification engines cannot determine issues with critical fields, such as a missing street suffix, a misspelled street name, or a city name (North Logan for Logan, Utah), that if standardized and corrected would result in more accurate matches and reduce the risk of untrusted IDs slipping through the cracks (Figure 8).

Figure 8: Melissa Returns Match Information on Many Attributes



Source: Melissa

MOBILE PHONE VERIFICATION

The identity verification challenge is not limited to onboarding. FIs also have multiple use cases that require the periodic scrubbing of existing customer data. A prime example is with the U.S. person-to-person payment service, Zelle. Zelle requires that FIs have a mobile phone number on file for all registered users, but many times FIs have no knowledge of whether the phone number they have on file for their customer is still valid, much less whether it's a mobile phone number. Melissa's expansive data assets, combined with its matching technology, can enable an FI to quickly screen its portfolio to determine what type of phone number is registered for the consumer—landline, mobile, or Voice over IP.

CONCLUSION

Financial services firms are facing a dual challenge of rapidly escalating financial crime and fierce competition in acquiring new customers. Here are a few recommendations for FI executives responsible for new-account acquisitions:

- **Create a delightful customer experience for your new applicants.** FIs are no longer just competing with each other; they're also competing with technology firms that have made digital transactions as easy and intuitive as possible for consumers. Look for solutions that can help resolve false positives early, minimizing their impact on the customer.

- **Look for providers with a solid track record in advanced matching routines.** Consumer data is messy, but providers that are experienced in applying advanced matching algorithms can spell the difference between a mountain of false positive alerts and a manageable number.

- **Find solution providers that have a global footprint.** The increasing globalization of commerce extends to banking, and banks need a better way to verify applicants who are new to the country.

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

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

Shirley Inscoe
+1.617.398.5050
sinscoe@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 MELISSA

Melissa is a leading global identity, entity resolution, and address verification company that provides solutions to instantly verify consumers and businesses online. Since 1985, more than 10,000 global customers, including financial service providers, e-commerce merchants, online gaming, and payment providers, have relied on Melissa for fraud prevention as well as AML and KYC compliance. Melissa's solutions offer unique and seamless integration into existing systems for fast, frictionless identity verification.

CONTACT

For more information about Melissa's products and services, please contact:

Melissa Sales
+1.800.MELISSA (635.4772)

sales@melissa.com