

# The Work Number ID: A Unique Approach to Identity Validation

MAY 2020

Prepared for:

**EQUIFAX**®

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	3
INTRODUCTION .....	4
METHODOLOGY .....	4
APPLICATION CHALLENGES .....	5
SYNTHETIC IDENTITY CHALLENGES .....	6
PORTFOLIO MANAGMENT .....	7
THE WORK NUMBER ID SOLUTION.....	8
HOW THE WORK NUMBER ID SOLUTION HELPS.....	8
THE WORK NUMBER ID VALUE-TEST RESULTS .....	8
CONCLUSION .....	10
ABOUT THE WORK NUMBER .....	11
CONTACT.....	11
ABOUT AITE GROUP.....	12
AUTHOR INFORMATION .....	12
CONTACT.....	12

## LIST OF FIGURES

FIGURE 1: CREDIT CARD APPLICATION APPROVAL RATES BY CHANNEL .....	5
FIGURE 2: LEADING PAIN POINTS IN FI FRAUD OPERATIONS.....	6
FIGURE 3: CREDIT CARD FRAUD LOSSES DUE TO USE OF SYNTHETIC IDENTITIES .....	7

## LIST OF TABLES

TABLE A: THE WORK NUMBER ID VALUE-TEST RESULTS .....	9
--	---

## EXECUTIVE SUMMARY

*The Work Number ID: A Unique Approach to Identity Validation*, commissioned by Equifax and produced by Aite Group, illustrates the value of being able to validate an identity with a single query as part of the application process.

Key takeaways from the study include the following:

- Validating identity by using data sourced from employment records at the time an applicant applies for credit can help eliminate fraudsters' use of synthetic identities.
- Verifying key personal information can assist in authenticating applicants more quickly.
- The application processes can be streamlined by first interrogating The Work Number database.
- The Work Number ID can add value across the life of a consumer relationship including scrubbing an account portfolio.

## INTRODUCTION

Financial institutions (FIs) face many challenges in today's market; one of the biggest is knowing who the consumer is on the other side of a telephone, computer, tablet, or desk. With the proliferation of fake IDs, a wealth of information available to fraudsters from numerous data breaches, and the creation of synthetic identities, fraudsters can overwhelm any FI's defenses. Consumers demand excellent service and want to apply for new cards and loans at their convenience—without having to go into a bank. Because using digital channels is less expensive for FIs than branches, this desire has all the potential for a real win-win for both consumers and FIs. The only problem? Knowing that the applicant is a real individual who exists in the real world.

This white paper focuses on the challenges FIs face in managing application fraud and in detecting applications from synthetic identities; it also presents information about a relatively new product that uses employment data as a way to validate identities of applicants for certain financial products and services. This paper will be of interest to all FI executives responsible for any type of application processing for new financial products.

## METHODOLOGY

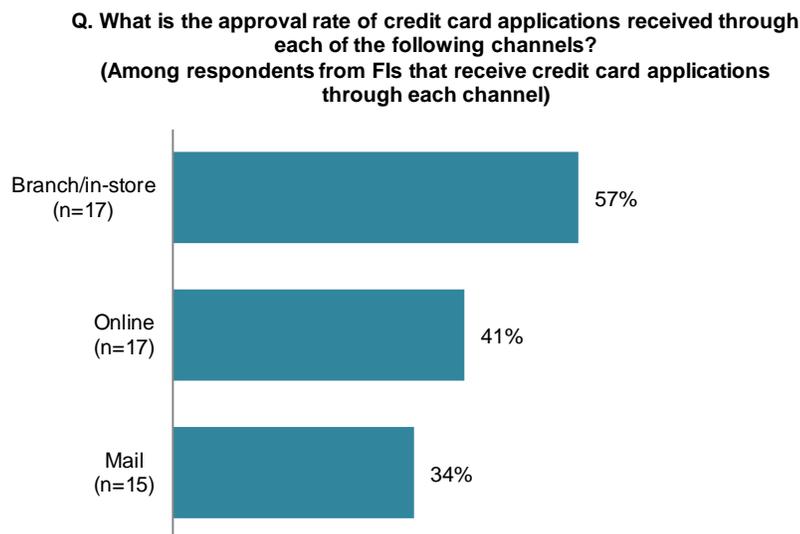
This white paper is based on research previously conducted by Aite Group on the challenges of application fraud and synthetic identities (current fraud challenges that FIs face), and on information about The Work Number ID solution provided by Equifax.

## APPLICATION CHALLENGES

FIs are in a fiercely competitive market trying to grow their business across all delivery channels. In particular, credit cards are being marketed very aggressively. FIs want to approve all applications possible while trying to avoid approving fraudulent applications to the extent possible and ensuring the consumers who are approved will handle their financial affairs responsibly.

Credit card applications taken in a branch environment are approved at a higher rate (57%) than those taken online (41%) or received via mail (34%).<sup>1</sup> In part, this may be due to branch personnel's ability to help consumers find a product they are more apt to qualify for, but it is also likely in part due to stronger fraud controls in the online channel. In any case, while approving all eligible applicants is the goal, declining potentially good applicants is a risk FIs must manage as well as possible as they attempt to control fraud losses (Figure 1).

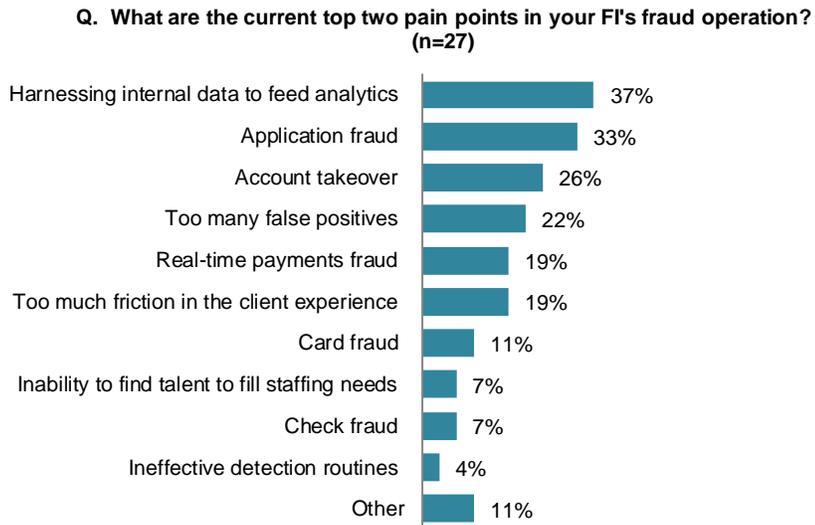
**Figure 1: Credit Card Application Approval Rates by Channel**



Source: Aite Group contactless card executive survey, October 2018 to March 2019

Unfortunately, the online channel has historically resulted in higher fraud rates than other delivery channels; thus, FIs tend to use stronger fraud controls online. Application fraud has become a leading problem for FIs in recent years and superseded account takeover fraud in 2019.<sup>2</sup> A full third of FI executives indicate that application fraud ranks in the top two pain points in fraud operations (Figure 2).

1. See Aite Group's report *Credit Card Account Opening and Onboarding: Metrics That Matter*, September 2019.
2. See Aite Group's report *Key Trends Driving FI Fraud Investments in 2020 and Beyond*, November 2019.

**Figure 2: Leading Pain Points in FI Fraud Operations**

Source: Aite Group survey of 30 financial fraud professionals, September 2019

Another costly aspect of trying to find the needles in the haystack that represent fraudulent applications are false positives—22% of executives name false positives as a top fraud pain point. Many good applications are identified as suspicious by fraud prevention systems, and analysts have to wade through all the alerts to identify the ones that truly are an issue versus those that are fine. This costs FIs both in the potential delay in approving good applications for consumers and the personnel and system expense of the fraud detection process.

## SYNTHETIC IDENTITY CHALLENGES

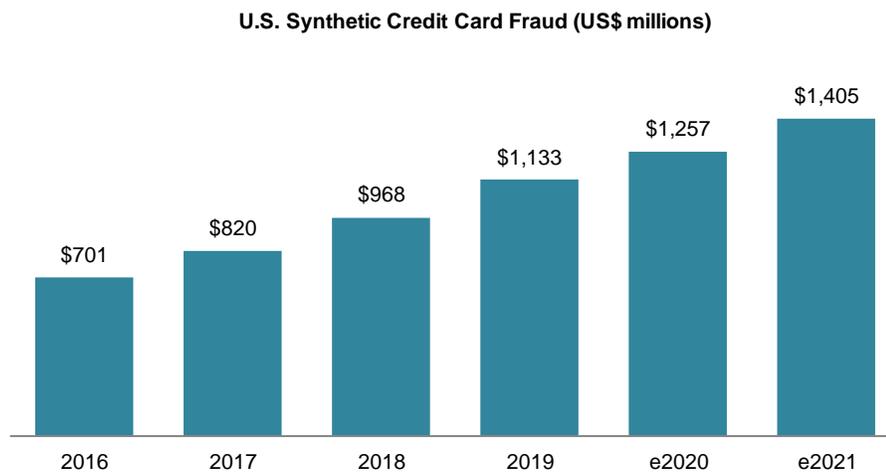
Synthetic or manufactured identities have been a challenge for many years—the financial services industry has yet to agree on a common definition for the term. As used for this white paper, the term “synthetic identities” includes all identities that are created partially or in total using fictitious data. In some cases, fraudsters will use certain fields of data from a real consumer; for example, they might use a legitimate Social Security number (SSN) and transpose some digits. Or, they might make up the data entirely; since the Social Security Administration began randomizing the assignment of SSNs in 2011, it has become much more difficult to detect whether any specific SSN is legitimate.

What is relatively new about the creation and subsequent use of synthetic identities is that fraudsters have begun creating large batches of such fictitious identities and creating real-world linkages for them. Typically, the first step is to obtain a mobile device in the newly created synthetic identity’s name. This provides an FI with the ability to contact the synthetic identity (i.e., the fraudster) after he or she applies for an account. Often, the second step is to create a credit file so the identity has a record with a credit reporting agency. To accomplish this, a fraudster may impersonate an existing customer and call to request that the synthetic identity be added to a credit card or a line of credit. After some period of time elapses, the synthetic

identity has a positive credit bureau record. Now, the fraudster can apply for credit cards or loans using the aged synthetic identities and most likely be approved—then use them for his or her nefarious activities.

Synthetic identities are a big problem that is continuing to grow, particularly with the aging of the identities that makes them so much more difficult to detect. For the credit card industry alone, Aite Group projects that fraud due to synthetics will grow to US\$1.4 billion by 2021 (Figure 3).<sup>3</sup>

**Figure 3: Credit Card Fraud Losses Due to Use of Synthetic Identities**



Source: Aite Group

## PORTFOLIO MANAGEMENT

Ideally, The Work Number ID would be used when a consumer first applies for a credit card or loan. Regardless of the quality of underwriting or application screening, some lenders may desire to use The Work Number ID to scrub a current account portfolio to ensure that previously booked loans have validated IDs.

Thus, The Work Number ID can add value across the life of a consumer relationship, not just at the application stage.

3. See Aite Group's report *Synthetic Identity Fraud: The Elephant in the Room*, May 2018.

## THE WORK NUMBER ID SOLUTION

The Work Number ID is a unique product that enables FIs to validate whether the name and SSN supplied by an applicant match a consumer's name and SSN in The Work Number database. Based on information returned from The Work Number ID service, the FI can determine whether any additional documentation is necessary from the applicant, possibly streamlining the application process and improving the customer experience. Information provided through The Work Number ID is a consumer report as defined under the Fair Credit Reporting Act (FCRA). Lenders must therefore have a permissible purpose to query The Work Number database to receive The Work Number ID solution. The database contains over 155 million identities and is always growing; the data is refreshed each pay period.

The Work Number ID will return one of three potential outcomes: Match (name and SSN), No Match (discrepancy in name), or No Hit (SSN not in database). For No Hit responses, FIs may continue to use their current process, but they can streamline the Match and No Match responses, reducing operational expenses related to that portion of applications. Applicants with Match responses (typically over 50%) should have an improved experience, making it less likely they will abandon the process.

## HOW THE WORK NUMBER ID SOLUTION HELPS

FIs often use third-party databases as they attempt to validate the identity of applicants for various financial products. The Work Number ID product is delivered from The Work Number, Equifax's database of employment and income information provided by employers and payroll processors across the U.S. The Work Number ID product will provide information to a lender as to whether the name and SSN provided by an applicant match a name and SSN in The Work Number database.

While fraudsters have figured out how to create virtual identities for their synthetics, it is much more difficult to make up an identity in the work world. Generally, synthetic identities do not hold down jobs or have real income. Thus, a query to The Work Number database can quickly help an FI assess whether it needs to collect more information when approving applications for financial products.

## THE WORK NUMBER ID VALUE-TEST RESULTS

In recent months, Equifax performed value tests with The Work Number ID solution and various customers with different use cases. The results of the value tests are summarized in Table A. The tests resulted in over 65% Match rates, with the highest reaching 87.64%. The No Match rates were single digits, with the lowest at 4.15%. Some types of product offerings will have higher Match rates than others; variances should be expected. Last, the No Hit rates ranged from roughly 8% to 30% in the three studies, but as Equifax adds data from more employers and payroll processors, these No Hit percentages should decline.

**Table A: The Work Number ID Value-Test Results**

Vertical	Approximate Number of records submitted by customer	Overall hit rate	Match percentage (name and SSN match)	No Match percentage (either name or SSN does not match)	No Hit percentage (SSN not in database)
<b>Consumer financing</b>	250,000	91.80%	87.64%	4.15%	8.21%
<b>Fintech company</b>	630,000	71.84%	67.42%	4.42%	28.16%
<b>Auto finance</b>	1,100,000	70.48%	65.01%	5.48%	29.52%

Source: Equifax

## CONCLUSION

Application fraud and the use of synthetic identities are two types of fraud providing tremendous challenges for FIs to manage. There is fierce competition among FIs for good customers, and fraudsters are constantly trying to represent themselves as potential good customers. Here are some key takeaways for consideration:

- When a consumer applies for credit, validating the information supplied by the applicant with The Work Number ID can help determine if the consumer is who they say they are, or if more information is needed about the consumer.
- Using The Work Number ID solution early in the application process may help eliminate the need for some of the existing tools and reduce total expense in validating identities.
- The Work Number ID solution can also be used to review a portfolio of consumer accounts having existing lines of credit.

## ABOUT THE WORK NUMBER

The Work Number is a proprietary database owned by Equifax, and it is the largest central source of commercial employment and income information. The database houses payroll information from hundreds of thousands of employers nationwide—from Fortune 500 companies to small regional and local employers—and fulfills millions of verifications each year for a variety of organizations.

Equifax is a global data, analytics, and technology company. Founded in 1899 and headquartered in Atlanta, Equifax operates or has investments in 24 countries in North America, Central and South America, Europe, and the Asia-Pacific region. Equifax employs over 10,000 people. It is a member of the New York Stock Exchange, and its stock is traded under the symbol EFX.

Equifax specializes in many areas, including risk modeling, credit reporting, marketing data, identity protection, HR compliance, employment verification, ACA compliance, technology, fraud prevention, artificial intelligence, machine learning, financial literacy, blockchain, cloud-based platforms, big data, trended data, data mining, cybersecurity, financial services, data analytics, cloud, and talent solutions.

## CONTACT

For more information about The Work Number solutions, email [info@theworknumber.com](mailto:info@theworknumber.com).

## 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](mailto:sinscoe@aitegroup.com)

## CONTACT

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

**Aite Group Sales**  
+1.617.338.6050  
[sales@aitegroup.com](mailto:sales@aitegroup.com)

For all press and conference inquiries, please contact:

**Aite Group PR**  
+1.617.398.5048  
[pr@aitegroup.com](mailto:pr@aitegroup.com)

For all other inquiries, please contact:

[info@aitegroup.com](mailto:info@aitegroup.com)