Aite PARTNER. ADVISOR. CATALYST.

Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise

FEBRUARY 2021

Julie Conroy

A complimentary copy of this Aite Group report is provided by:

TransUnion

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

IMPACT POINTS

- Synthetic identity fraud is a pernicious issue that results when criminals fabricate identities to establish new accounts or lines of credit and use those fake identities to steal or move money. While financial services firms are certainly a key target of these attacks, a number of other vertical markets also feel the pain of synthetic identity fraud, including property rentals, utilities, telecom, and gambling.
- This report, sponsored by TransUnion, examines synthetic identity fraud's impact and best practices in combating the issue. To inform the research, Aite Group surveyed 46 North American fraud executives in September 2020. The report also includes input and insights from ongoing Aite Group conversations with fraud executives at financial institutions (FIs) and fintech lenders.
- Seventy-two percent of financial services firms surveyed believe that synthetic identities are a much more challenging issue to identify and address than identity theft.
- The majority of financial services firms recognize that they have significant gaps in their application fraud control framework, and 78% of executives surveyed plan to make substantive changes in the next one to two years.
- While most of the executives surveyed believe that the Social Security Administration's (SSA's) electronic Consent Based Social Security Number Verification (eCBSV) program will be a helpful tool, it will not be a silver bullet. The lack of fuzzy matching is a key concern; executives expect high levels of false positives as a result.
- Data exchanges and consortia are the most highly favored solutions by survey respondents; 82% believe them to be highly effective or effective when combating synthetic identity fraud. Third-party analytic models are a close second, with 72% of executives deeming these to be highly effective or effective.
- Aite Group estimates that synthetic identity fraud for unsecured U.S. credit products will reach US$1.8 billion in 2020 and will grow to US$2.42 billion in 2023.

INTRODUCTION

Synthetic identity fraud is a pernicious issue that results when criminals fabricate identities to establish new accounts or lines of credit and use those fake identities to steal or move money. Synthetics are hard to detect; most companies don't realize the full extent of their exposure, because synthetic attacks are often written off as credit losses (thus the moniker "diabolical charge-offs").

The U.S. market is one of the hotbeds of synthetic identity fraud, given the historical lack of a centralized source of truth for consumers' identities. The topic has been gaining increasing scrutiny over the past few years. Many firms are investing in technologies to help better identify synthetic fraudsters at the time of application, as well as find those lurking in existing portfolios. Regulators and legislators are focusing on the issue as well. The U.S. Federal Reserve launched an initiative in 2018 to raise the industry's awareness of the risks of synthetic identities. That same year, the U.S. Congress passed a bill requiring that the SSA enable a real-time service that allows authorized firms to verify an applicant's name, Social Security number (SSN), and date of birth. The resulting eCBSV program was slated to launch its pilot phase in June 2020, but the pilot has struggled to get off the ground.

This Impact Report defines synthetic identity fraud, sizes its impact on the U.S. unsecured credit market, and discusses best practices in addressing the growing problem of synthetic identity fraud.

METHODOLOGY

This report, sponsored by TransUnion, examines synthetic identity fraud's impact as well as firms' current and planned approaches to combating the issue. To inform the research, Aite Group surveyed 46 North American fraud executives in September 2020. The report also includes input and insights from ongoing Aite Group conversations with fraud executives at FIs and fintech lenders.

WHAT IS SYNTHETIC IDENTITY FRAUD?

The question "What is synthetic identity fraud?" is not straightforward. While various types of card fraud are well-defined by the payment networks, there is no common industry definition for synthetics, which makes it difficult to detect, benchmark, and address. The variations of synthetic identity fraud fall into a few common buckets (Table A).

Table A: Synthetic Identity Definitions

Type	Definition
Identity fabrication	The identity is generated out of the ether, not using any genuine identity data elements.
Identity manipulation	Genuine identity data elements are tweaked slightly to create a new identity.
Identity compilation	Bits and pieces of different stolen identities are compiled to form a new identity (aka Frankenstein fraud).
Credit profile number	The credit profile number is a nine-digit number that is sold by credit repair agencies to consumers with bad credit to "get a fresh start." It is also often used by illegal immigrants to access credit. The intent is to obfuscate creditors' inquiries to credit bureaus and establish new records for the consumer.

Source: Aite Group

While FIs and fintech lenders represent particularly attractive targets for these attacks, the impact is by no means limited to these verticals. A wide variety of vertical markets are impacted by synthetic identity fraud:

- **Rental screening:** Rental properties are often targeted with a variety of forms of identity fraud, including synthetics. It is very costly and time consuming for a landlord to evict a tenant, so catching fraud at the front door is critical in this market.
- **Utilities:** As crime rings set up shop, most are not inclined to pay to keep the lights on out of their own pocket when they can leverage stolen and synthetic identities to set up the utility accounts.
- **Telecom:** With very low churn rates and competition fierce for new customers, the barriers to entry to obtain a new mobile phone account are often relatively low. Mobile phone accounts are often a key underpinning of a synthetic identity. The telecom firm reports the account to credit bureaus, thus further establishing the authenticity of the fake identity, but then as credit-granting institutions leverage mobile network operator data as part of their authentication process, the established mobile phone account in the name of the synthetic identity helps the fake account sail through with flying colors.
- **Gambling:** Stakes are high in faceless gambling, and synthetic identity fraud follows the dollars. Gambling sites are a key target for synthetic fraud rings, as they seek to

leverage carefully nurtured identities, often combined with stolen payment card information.

HOW TO ESTABLISH A NEW IDENTITY

While synthetic identity fraud is by no means limited to the U.S., the problem is particularly painful in that market, given the lack of source data that can verify an individual's identity. Due to U.S. regulations, credit bureaus may not use a consumer's SSN as their primary key for the credit record. Instead, they have proprietary matching processes to determine whether the individual has a credit record or whether a new record should be established. This matching process attempts to account for the fact that data furnishers often do not submit perfect data—there are often mistakes in the furnished data, such as fat-finger errors, old addresses, and name changes.

Organized crime rings understand this and capitalize on the gaps in the system to successfully create a new identity and establish it as a creditworthy entity. The rings build a new identity in a few key ways (Table B). While the first application for credit using a newly minted synthetic identity will often be declined due to lack of verifiable history, that is enough to establish a foothold, and the second and third attempts will find a credit grantor willing to take a chance on this "thin file" applicant. Many of the actions in Table B are taken in parallel, then repeated over time to build the new identity's creditworthiness.

Table B: How to Establish a New Identity

Method	Description
Add an authorized user to an existing credit line	Criminals add the new identity as an authorized user to an existing line of credit. FIs often don't do the same level of due diligence when adding an authorized user to an established trade line since the primary user is ultimately responsible for the debt, and FIs typically see a 30% increase in spending when an authorized user is added to the account. The authorized user gets reported to the credit bureau, thus serving as the entry point for the new identity.
Apply for a rental property	Not only does this provide the fraudster with an operational base (at a low cost, since at some point the bust-out will occur and the landlord will be left with a number of months' rent due), but it also further reinforces the veracity of the fake identity.
Apply for a secured credit card	A secured card is a financial product for consumers looking to build or rebuild credit, whereby the consumer pays a cash deposit that becomes the line of credit. Because of the deposit, FIs have little financial exposure, so they often don't put the same level of rigor into underwriting and risk assessment. The credit history is submitted to the bureaus, however, which serves as another potential foothold for the synthetic identity.

Method	Description
Get a mobile phone	U.S. mobile carriers have a sub-1% churn rate, so competition for new customers is intense, and the barriers to entry for a new identity are relatively low. The mobile phone not only further establishes activity history for the identity but also helps the fraudster pass stepped-up authentication, such as inquiries to the mobile network operator to determine whether the identity is associated with the phone number and SMS one-time passwords.
Social media presence	Fraudsters understand that FIs often evaluate the applicant's social media presence as part of the fraud risk-assessment process. More sophisticated criminals set up social media profiles for the synthetic identity and nurture it for months or years.
Complicit data furnisher	While a more complex entry point, there have been cases of internal fraud or fraudulent businesses set up to furnish data to the bureaus and establish new synthetic identities. This attack method is particularly prevalent in auto finance.
Slow-and-steady credit building	Sophisticated fraudsters are aware that the entry method of an authorized user is increasingly scrutinized, so they build their new identities patiently over time, emulating the behavior of a genuine consumer that is new to credit or new to the country.

Source: Aite Group

Children's SSNs are especially vulnerable to synthetic identity fraud. Because children cannot actively apply for credit until age 18, criminals use their stolen SSNs for years without detection. The elderly also are susceptible, since they often are not in the market for new lines of credit and thus are less vigilant about unauthorized use of their identity.

ANATOMY OF A SYNTHETIC FRAUD ATTACK

A September 2020, U.S. federal indictment of participants in a coordinated synthetic identity fraud attack illustrates the extent to which the crime rings behind these attacks play the long game (Figure 1).[1] The ring included 13 individuals and three fraudulent businesses and, over the course of 18 months, obtained more than US$1 million in fraudulent loans from 19 U.S. banks and credit unions:

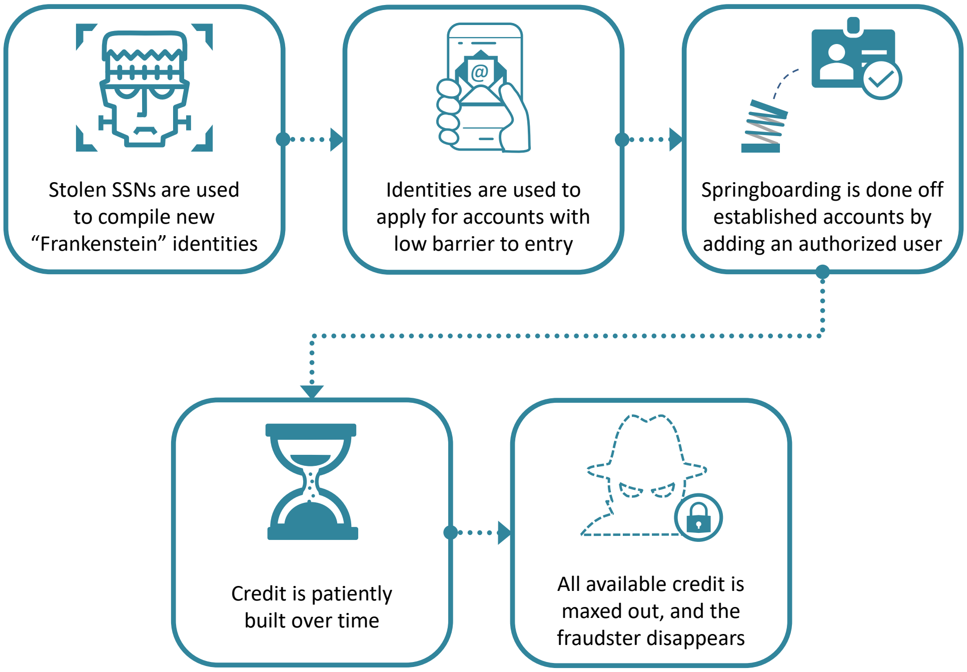
- Twenty synthetic identities were compiled using SSNs stolen from individuals unlikely to be accessing credit—children, incarcerated people, and elderly individuals—and the fraudsters then appended new names, addresses, dates of birth, etc.

- The fraudsters proceeded to apply for accounts with minimal identity verification requirements—email accounts, mobile phones, and loyalty points to give the identities a foothold.

[1] "13 Individuals and 3 Corporations Indicted for Alleged Nation-Wide Synthetic Identity Scheme," Suffolk County District Attorney, September 23, 2020, accessed October 27, 2020, https://www.suffolkcountyny.gov/da/News-and-Public-Information/Press-Releases/13-individuals-and-3-corporations-indicted-for-alleged-nation-wide-synthetic-identity-scheme.

- The fraudsters then used the tried-and-true tactic of springboarding—i.e., adding synthetic identities to existing established credit card accounts as authorized users. The ring also created shell companies that were used to report credit history on the synthetic identities (backdated in some cases, to further add validity).
- The ring patiently nurtured the identities for more than a year, paying bills on time and gradually adding lines of credit, before finally maxing out all of the credit lines and busting out.

Figure 1: Anatomy of a Synthetic Fraud Attack

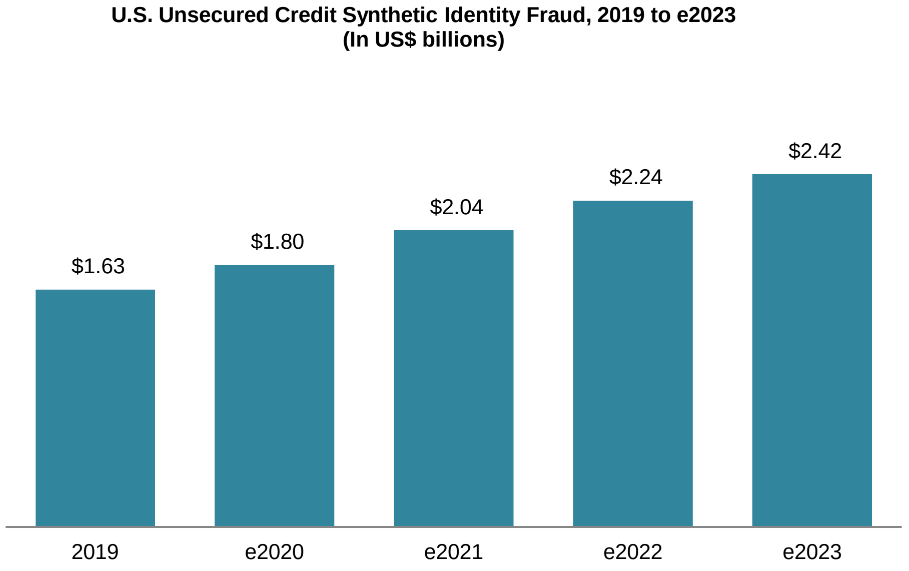

Stolen SSNs are used to compile new "Frankenstein" identities
Identities are used to apply for accounts with low barrier to entry
Springboarding is done off established accounts by adding an authorized user
Credit is patiently built over time
All available credit is maxed out, and the fraudster disappears

Source: Aite Group

MARKET TRENDS AND SIZING

Given the porous nature of the identity framework in the U.S. market, synthetic identity fraud continues to rise. Based on ongoing discussions with U.S. financial services firms, Aite Group estimates that synthetic identity fraud for unsecured U.S. credit products will total US$1.8 billion in 2020, and it will grow to US$2.42 billion in 2023 (Figure 2). These estimates are conservative—if the amount of credit charge-offs attributable to synthetics are indeed universally in the 10% to 15% range, as indicated by some of the issuers and lenders interviewed for this report, then the losses could be as high as US$6 billion.

Figure 2: U.S. Unsecured Credit Losses Due to Synthetic Identity Fraud



Source: Aite Group

Table C summarizes key trends around synthetics and the resulting market implications.

Table C: Synthetic Identity Fraud: Market Trends and Implications

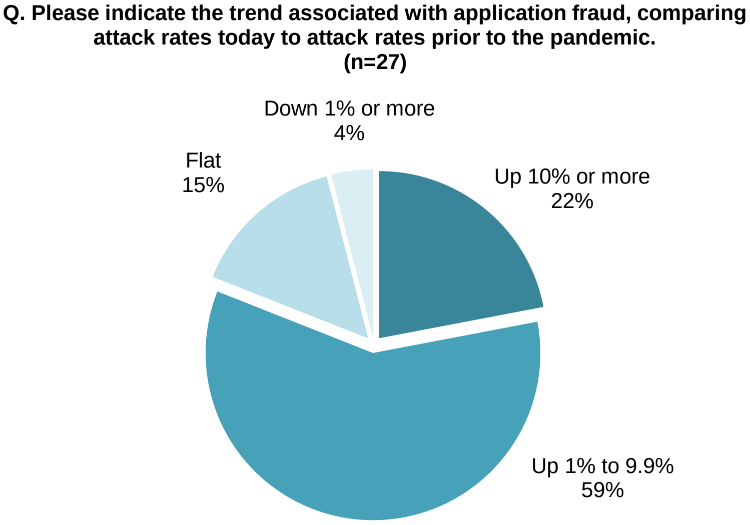
Market trends	Market implications
Synthetic identity fraud continues to rise; many firms are just beginning to understand the extent of the issue.	A perfect storm formed around synthetics in the early half of the 2010s, and fraudsters have been capitalizing ever since. More than 30 billion data records have been breached since 2013, placing plenty of raw material for compiling Frankenstein synthetics in fraudsters' hands. The SSA began randomizing the issuance of SSNs in 2011, eliminating the ability for credit grantors to use the chronological logic inherent in SSN issuance to flag potential risk. And most of the global economy enjoyed steady growth during the 2010s, making it easier to establish new identities as lenders competed for new business.
Regulators and legislators are also focusing on synthetics.	Synthetic identities are not just a fraud or credit risk issue; they represent a Know Your Customer (KYC) issue as well. A firm with a large number of synthetics on its books obviously doesn't "know its customers," and the problem of synthetics is increasingly on regulators' radar.
No silver bullet exists for synthetics—detection and remediation require a layered approach.	Firms are increasingly looking to put stronger controls around the application as well as an account's early life to detect synthetics. This requires a layered approach, analyzing both static personally identifiable information and digital identity elements.

Source: Aite Group

SYNTHETICS: AN INCREASING ISSUE

Application fraud has been a particularly acute pain point for financial services firms in the wake of the COVID-19 pandemic. Fraudsters quickly capitalized on the easy opportunity to steal funds from governmental unemployment and small-business lending stimulus programs. They then used stolen and synthetic identities, as well as mule recruitment schemes, to exit the funds from the financial system. As a result, 81% of FIs surveyed say that application fraud has increased in the wake of the pandemic (Figure 3).

Figure 3: The Pandemic Drove a Sharp Increase in Application Fraud

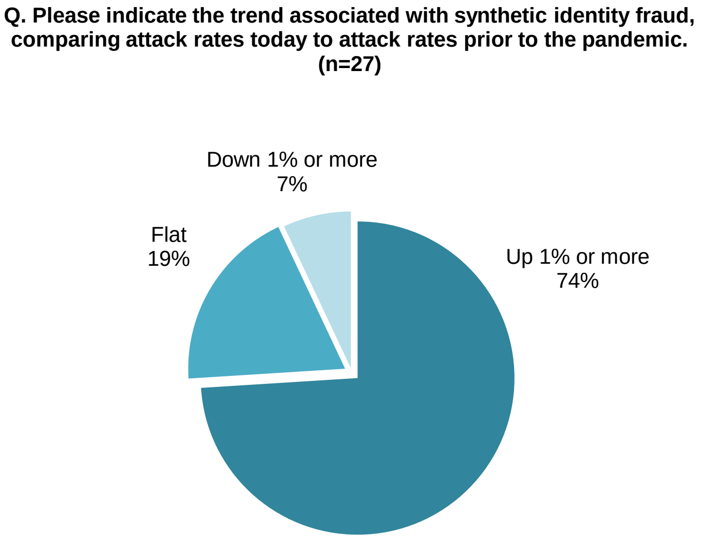


Source: Aite Group survey of 46 financial services fraud executives, September 2020

Synthetic identity fraud represents a subset of overall application fraud. Most FIs say that identity theft has been an acute pain point in 2020, as crime rings file for unemployment on behalf of an unwitting victim and then open an account in the name of that individual to receive the unemployment benefits. That said, mule accounts are a key mechanism to exit those stolen funds from the financial system, and the industry has also seen a massive uptick in account openings related to mule activity. Account opening related to mule accounts manifests as first-party fraud (consumers who are duped by romance or work-from-home scams), identity theft, and synthetic identities.

Given the economic downturn that has accompanied the pandemic, many credit card issuers and consumer lenders have curtailed marketing activities and tightened their credit issuance policies. With all of these factors, it is no surprise that on a rate basis, 74% of respondents have seen synthetic identity fraud also increase in 2020 (Figure 4).

Figure 4: The Synthetic Fraud Rate Is Also Rising

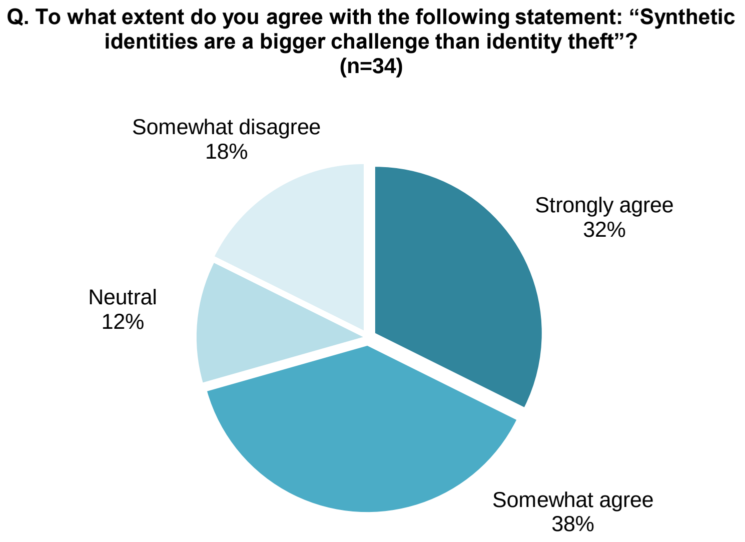


Source: Aite Group survey of 46 financial services fraud executives, September 2020

Synthetic attacks vary in methodology. Fintech lenders see smash-and-grab attacks—attackers maximize their opportunity at the point of application, since that is when the credit decision and near-real-time funding happens. In contrast, synthetic attacks on credit card and demand deposit accounts tend to include patient nurturing of the identity and expansion of the relationship (i.e., steadily increasing lines of credit) anywhere from six months to five years or more. Synthetic identity fraud is by no means limited to financial services, either—online gaming and telecom firms see high attack rates as well.

The vast majority of FIs surveyed (70%) believe that synthetic identities are a much more challenging issue than identity theft (Figure 5). It is difficult to differentiate a synthetic identity from an applicant new to credit or new to the country. The crime rings behind the bulk of the fraud are patient and will often build up synthetic credit lines over months or years before they bust out. Once on the books, synthetics are often written off as credit losses. This represents a double whammy for the credit grantor; not only does it absorb the loss, but it also expends valuable resources trying to collect from someone who doesn’t exist.

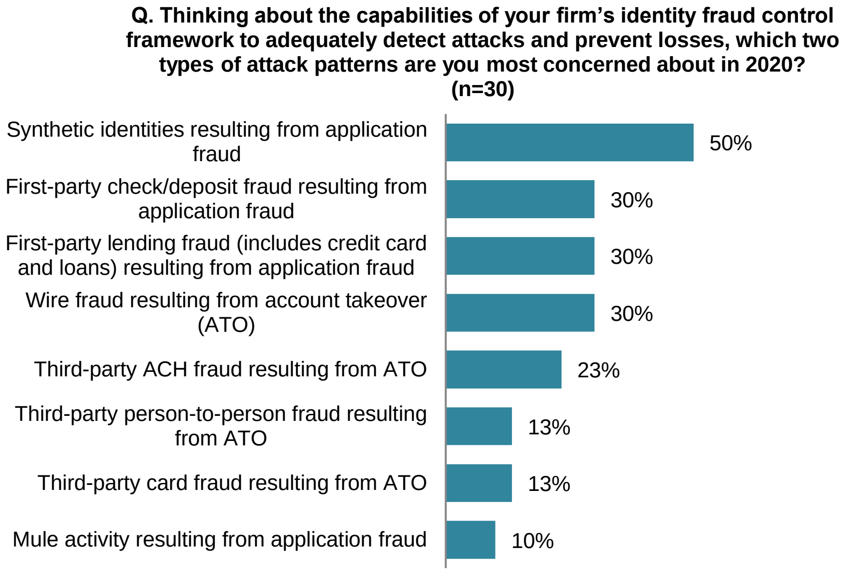
Figure 5: Synthetics Are Challenging to Detect



Source: Aite Group survey of 46 financial services fraud executives, September 2020

Aite Group asked fraud executives about their confidence in their control framework's ability to detect attacks and prevent losses across a variety of fraud types. As shown in Figure 6, FIs are disproportionately concerned about synthetic identity fraud relative to other fraud types. Half of respondents indicate that synthetic identities are among their top two points of concern. This is likely due to the difficulty of identifying synthetics, plus the relatively large magnitude of the losses if sleeper synthetics have been nurtured for months or years.

Figure 6: Synthetic Identity Fraud Is a Key Point of Vulnerability

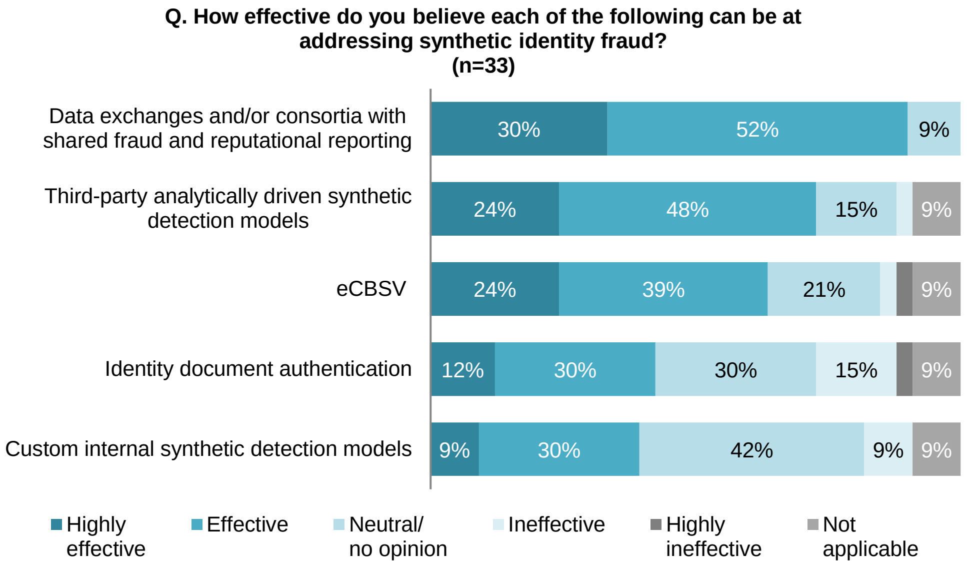


Source: Aite Group survey of 46 financial services fraud executives, September 2020

TECHNOLOGY TO THE RESCUE

While there is no silver bullet, a variety of solutions can help with the synthetic problem (Figure 7). Data is the friend of anyone looking for synthetics, either at the time of account opening or within a portfolio. Data exchanges and consortia are the most highly favored solutions by survey respondents; 82% believe them to be highly effective or effective when combating synthetic identity fraud. Third-party analytic models are a close second, with 72% of executives deeming these to be highly effective or effective.

Figure 7: Various Solutions Can Assist



Source: Aite Group survey of 46 financial services fraud executives, September 2020

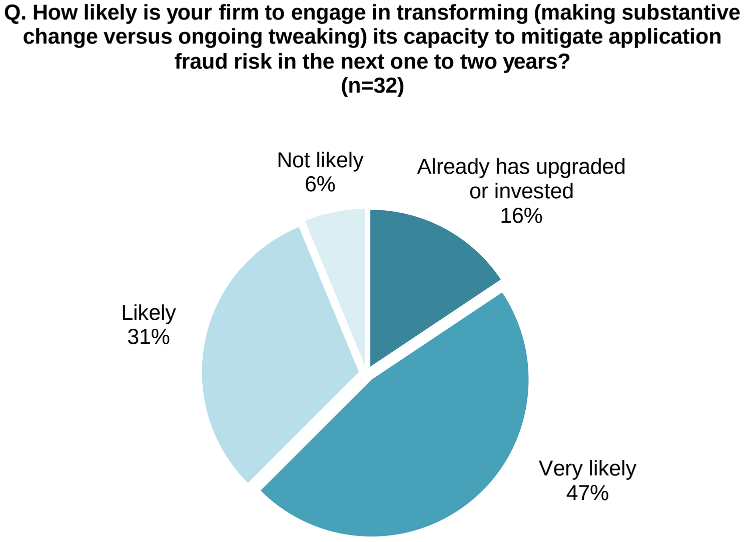
The following describes various control mechanisms in greater detail:

- **Data exchanges and consortia:** Consortia-based databases are a great way for businesses to share intelligence about identity-data-associated fraud losses. Consortia-based intelligence comes in a couple of different flavors:
    - **Fair Credit Reporting Act (FCRA)-compliant:** Businesses using FCRA-compliant services can decline accounts based on the data within the services. Firms contributing data to FCRA-compliant databases must be able to support a process that gives the consumer the opportunity to dispute the contributed record.
    - **Non-FCRA:** The reputational data in non-FCRA services is purely intended as a risk flag—businesses are not permitted to deny services based solely on the reputational risk flags, since there is no adverse action process. Device identity consortia was cited as an important input into synthetic detection routines by executives interviewed for this report.

- **Third-party analytically driven models:** Seventy-five percent of FIs interviewed believe that third-party analytically driven models are either highly effective or effective against synthetics. These can include many external inputs to facilitate analysis of the consistency of a consumer's identifying data. For example, how old is the person, when did the consumer's credit bureau history first appear, how far back does their address history go, how old were they when they got their SSN, and how old was the person when they first accessed credit? Taken in conjunction, this type of analysis can help flag potential synthetics at the time of application, as well as those lurking within existing portfolios.
- **ECBSV:** While 63% of executives surveyed are optimistic about the eCBSV's potential, it will not be a silver bullet. The system's lack of fuzzy matching means that there will be a high false-positive rate. Substantial concern exists about the system's scalability as well—it will likely be quite some time before the eCBSV can handle the volume at scale with the required response times for account onboarding. The planned approach to using the eCBSV varies among firms interviewed. Some plan to send 100% of their application volume (some in real time, others offline), while others plan to just send a subset due to cost and manual review considerations.
- **Identity document authentication:** While fake identity documents are readily available on the internet, it's more difficult to get a driver's license or passport that has all of the appropriate security features embedded (e.g., holograms, microprints, bar codes). Using document authentication as part of the onboarding process can help detect the fake applicants and can also help streamline the onboarding process by using the data to auto-populate application forms.
- **Custom internal synthetic models:** Just 42% of the executives surveyed believe that internally developed synthetic models are a highly effective or effective countermeasure. A key driver behind this is attributable to FIs' historical gap in their ability to accurately identify and tag synthetic identity fraud. One of the FI executives interviewed says that his fraud prevention team began this tagging two years ago, but at the time did not include the FI's credit risk business partners. In retrospect, that created a big gap in the process, since a number of synthetics were missed.

The good news is that the majority of FIs recognize that they have significant gaps in their application fraud control framework, and 78% of executives surveyed plan to make substantive changes in the next one to two years (Figure 8).

Figure 8: Changes Are on the Horizon



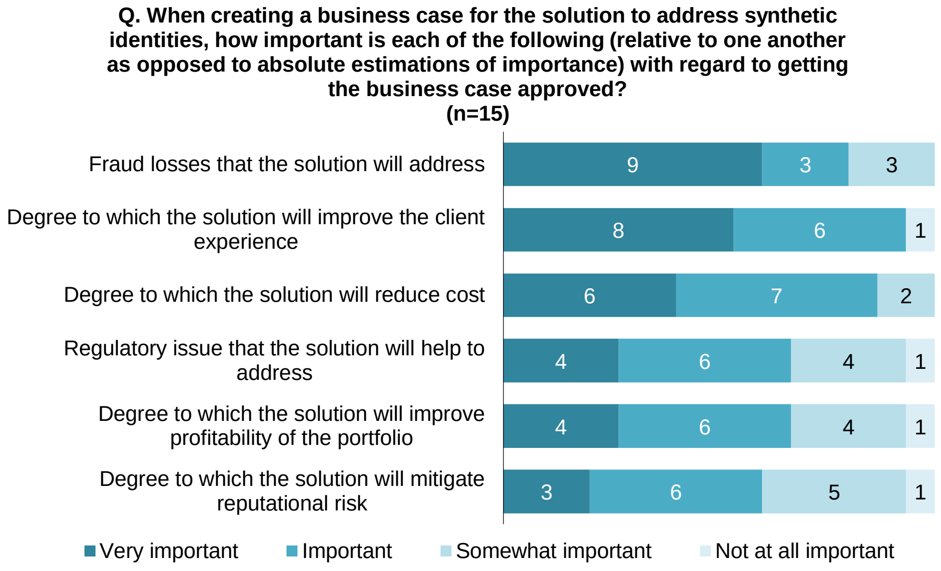
Source: Aite Group survey of 46 financial services fraud executives, September 2020

When it comes to making the business case to address synthetic identity fraud, a number of important factors come into play (Figure 9):

- **Fraud losses:** Given the vast amount of synthetic fraud that is lurking in credit losses, reining in fraud losses is a key priority for the majority of firms surveyed.
- **Customer experience:** Aite Group research consistently finds that enhancing the customer experience ranks as one of the top business case drivers for new investments in the fraud and authentication control framework, and synthetics are no exception.
- **Cost reduction:** Cost reduction is always a goal of financial services firms, but it is particularly important during economic downturns. Through better detection of synthetic identity fraud at the front end of the customer life cycle, firms can keep those losses from going into collections queues, which wastes valuable full-time employees' time trying to collect from someone who doesn't exist.
- **Regulatory considerations:** The recent focus on the synthetic identity fraud by the U.S. Federal Reserve signals that this issue is very much on regulators' radar. This indicates that it will increasingly be viewed as a KYC issue that will be scrutinized by regulators during periodic anti-money laundering compliance exams.
- **Portfolio profitability:** Profitability is a key metric for any ongoing concern, so best-in-class solutions will be those that can help increase revenue (by better reducing false declines at the time of onboarding), as well as optimize efficiency through a low false-positive rate.
- **Mitigate reputational risk:** While this is not a primary business case driver for most of the respondents, financial services firms never like to have their brand hit the

headlines in conjunction with fraud or money laundering issues. A proactive stance against synthetics can help firms avoid being attached to news stories such as the one cited in this report.

Figure 9: Business Case Drivers for Synthetic Identity Fraud Investments



Q. When creating a business case for the solution to address synthetic identities, how important is each of the following (relative to one another as opposed to absolute estimations of importance) with regard to getting the business case approved?
(n=15)

Source: Aite Group survey of 46 financial services fraud executives, September 2020

CONCLUSION

Synthetic identity fraud is a pressing concern for any firm that is extending actual or provisional credit to consumers. Here are a few recommendations for firms as they seek to evolve their control framework to better address the challenge of diabolical charge-offs:

- **Apply a multipronged detection strategy.** As with most types of fraud, there is no silver bullet for synthetic identity fraud. Financial services providers need to combine the analysis of credit file data, public record data, and digital identity data to effectively detect potential synthetic identities.

- **Segment the remediation approach for suspected synthetic fraud.** Once fraud is detected, credit grantors need a segmented remediation process for synthetic versus third-party fraud, since the criminals who take the time to cultivate synthetic identities are often able to effectively navigate traditional stepped-up authentication processes.

- **Analyze collections queues.** Many synthetic identities are written off as credit losses. Credit issuers should analyze their existing credit write-offs to determine what proportion of them are synthetic. Not only will this help better inform analytic routines to help detect future synthetic fraud, but it also will remove the synthetic identities from collections queues, thus freeing up valuable resources to focus on recovery opportunities.

RELATED AITE GROUP RESEARCH

Application Fraud: Accelerating Attacks and Compelling Investment Opportunities, November 2020.

Aite Group's Third Annual Financial Crime Forum: Collaboration Amid Crisis, October 2020.

Fraud, Authentication, and Orchestration Hubs: A Path to Greater Agility, December 2019.

Key Trends Driving FI Fraud Investments in 2020 and Beyond, November 2019.

Unsecured Lending: New Opportunities for Credit Issuers…and Fraudsters, January 2019.

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

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