Aite PARTNER. ADVISOR. CATALYST.

The Dreaded Trinity of Identity Theft, Application Fraud, and Account Takeover

APRIL 2021

Prepared for:

Accertify
AN AMERICAN EXPRESS COMPANY

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Dreaded Trinity of Identity Theft, Application Fraud, and Account Takeover, commissioned by Accertify and produced by Aite Group, examines trends in identity theft, application fraud, and account takeover. It reveals insights into how these criminal activities relate to one another and impact financial services providers, merchants, and any company that has an interest in managing the security of customer accounts.

Key takeaways from the study include the following:

- Market forces have been driving growth in identity theft for years, but the environmental conditions of the pandemic have accelerated this growth in the past year.
- Application fraud is the practice of using stolen or synthetic identity information to set up an account that the perpetrator uses to support criminal activity for personal gain. The incidence rate of application fraud has increased in proportion to the incidence rate of identity theft, according to Aite Group's 2021 consumer research.
- Account takeover is the practice of using stolen identity information to deceive an institution into surrendering control over the account to an unauthorized user. It has also increased proportionally to the incidence rate of identity theft as reported by consumers.
- While financial services firms are the most common targets of application fraud and account takeover attacks, fraudsters also attack merchants, hospitality companies, travel companies, government agencies, and any institution charged with protecting customer accounts designed to manage cash or cash equivalents.
- As attack rates have increased, so too has pressure from consumers to step up security measures without creating additional friction in the user experience.

INTRODUCTION

The term "identity theft" is in wide circulation, and the concept has received an increasing amount of public attention. Most fraud executives understand identity theft to be the upstream root cause of a growing range of fraud types generically categorized as identity fraud. The two most common forms of identity fraud—application fraud and account takeover—are themselves categories of a variety of subordinate types of fraud attacks that have been among the fastest-growing forms of fraud plaguing whole sectors of the economy, including financial services, retail, hospitality, travel, and even government.

The increasing incidence rate of identity theft and the expanding portion of the public who have fallen victim to it have driven public demand not only for analysis into the size and scope of the challenge but also for insights into the kinds of criminal activity that result from it. This white paper, commissioned by Accertify, an American Express company, examines trends in identity theft as reported by a survey of more than 8,000 adults in the U.S. It analyzes how those trends align with trends in application fraud and account takeover reported by fraud executives in 2020. Insights from this white paper will be of interest to fraud executives and solution providers in the anti-fraud marketplace, and to readers who are eager to better understand the interrelationship between identity theft, application fraud, and account takeover.

METHODOLOGY

Data for this white paper were gathered from an online quantitative survey in December 2020 and from a survey of 47 fraud executives who attended Aite Group's Financial Crime Forum in September of 2020. The consumer survey gathered responses from 8,653 U.S. consumers aged 18 or older. Of those, 4,101 (47%) experienced financial identity theft. To create an accurate market profile of financial identity theft, the sampling was click-balanced to the U.S. census for age, gender, income, and region.

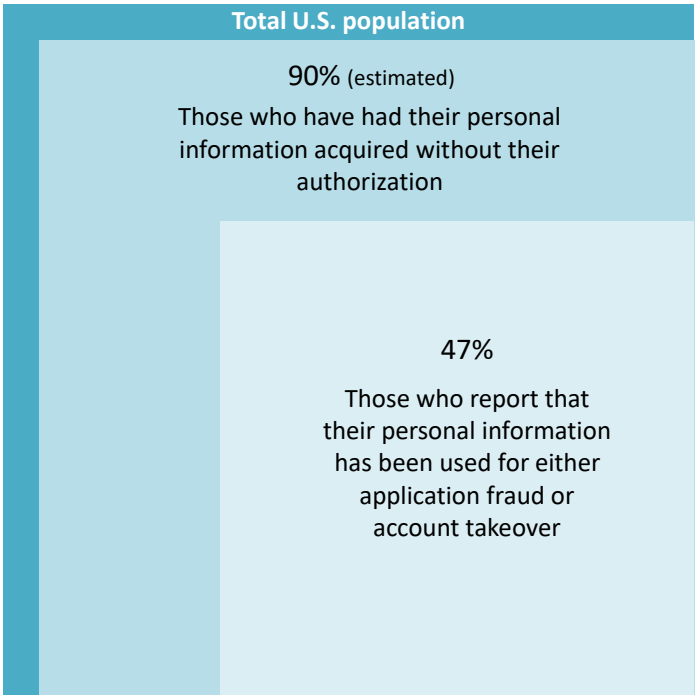
The data from the consumer study have a margin of error of approximately 3 points at the 99% confidence level, while the findings from the fraud executives can be considered a directional indication of conditions in the market. Statistical tests of significance between groups, where shown, were conducted at the 99% level of confidence. In addition, research examined how the COVID-19 pandemic influenced many consumers to change ingrained banking behaviors.

IDENTITY THEFT: THE DRIVING FORCE

The topic of identity as it relates to fraud is an exceptionally complex issue and is made so by dint of the wide variety of concepts, definitions, and trends in this arena. The objective of this white paper is to examine recent trends in identity theft and the criminal activity that stems from it in order to understand the scope of its impact on consumers and the institutions that are struggling to manage it. As is almost always the case when discussing complex matters such as this, it's helpful to set a foundation with some definitions.

The term "identity theft" is defined by Aite Group as the fraudulent acquisition and use of a person's personally identifying information (PII), usually for financial gain. The noteworthy phrase in the definition is "fraudulent acquisition and use," which means that the perpetrator obtained the PII by way of intentional deception. Also helpful is the manner in which the definition breaks the criminal act out into two discrete stages. The first stage, the acquisition of the victim's PII, is a requisite precursor to the second stage, usually the use of the victim's PII for financial gain. Breaking the criminal act down in this manner illustrates the size and scope of who is impacted by identity theft. Under this conceptual model of identity theft, it's possible to visualize the distribution of various segments of the population in terms of how they are impacted by identity fraud (Figure 1).

Figure 1: Conceptual Model for Visualizing the Distribution of the Impact of Identity Theft

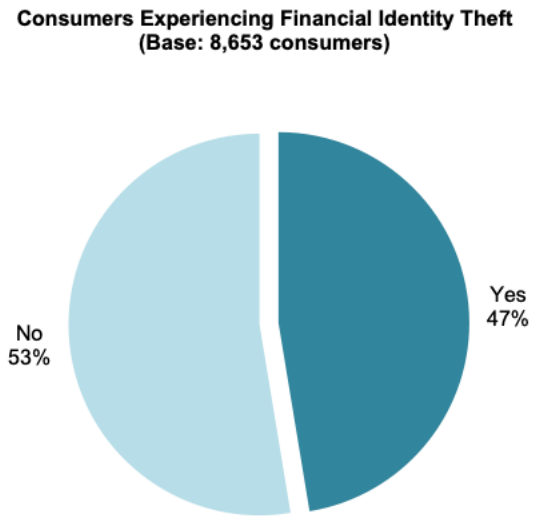


Source: Aite Group

There are, of course, several reliable estimates for the superset population—the total U.S. population. The United States Census Bureau estimates that there were 330 million people in

the country as of July 2020.[1] Controlling for only adult-aged individuals leaves 255 million people.[2] Aite Group's consumer survey on identity theft collected responses from 8,653 U.S. consumers aged 18 or older. Of those, 4,101 (47%) experienced financial identity theft (Figure 2). Extrapolating the percentage of identity theft victims from the consumer research to the total adult population yields an estimate of just under 120 million adult-aged residents of the U.S. who would be aware that their PII has been used without consent.

Figure 2: Identity Theft Victims in the Past Two Years



Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Of the three population segments of the identity theft model, the one that is widely reported but reveals little in the way of a consistent estimate is the total number of people whose PII has been fraudulently acquired. This is partly because the majority of thefts of this information take the form of large-scale data breaches, and the preferred means of measuring the impact of these data breaches is to count the total number of records exposed. While records often correlate to a discrete individual, the companies that disclose these breaches rarely disclose the rate of correlation of records to individuals. As a result, estimating the total number of individuals whose PII has been fraudulently acquired remains more of an educated guess.

1. Eric Jensen, "Demographic Analysis Uses Birth and Death Records, International Migration Data and Medicare Records to Produce a Range of Population Estimates as of April 1, 2020," United States Census Bureau, published December 14, 2020, accessed March 3, 2021, https://www.census.gov/library/stories/2020/12/census-bureau-provides-population-estimates-for-independent-evaluation-of-upcoming-census-results.html.

2. "National Population by Characteristics: 2010-2019," U.S. Census Bureau, accessed March 10, 2021, https://www.census.gov/data/tables/time-series/demo/popest/2010s-national-detail.html.

Largely out of an abundance of caution, most leaders of fraud management units in the financial services industry operate on the assumption that everyone's PII has been exposed. While that's a possibility, it's difficult to imagine a scenario in which fully 100% of the population has had their PII exposed by fraudulent means. But data breaches have reached such a frequency and level of severity that an overwhelmingly large percentage of the total population has been exposed. One need not look too far for evidence in support of this. Consider that just one data breach event in recent history released the PII of more than 147 million people, or roughly 45% of the U.S. population.[3] So while the number isn't likely to be a full 100% of the population, based on the frequency, severity, and persistence of major data breaches over the past 10 years, it is probably safe to assume that the number would be in the neighborhood of 90% or more of the U.S. population aged 18 years or older, or just under 230 million people.

IDENTITY THEFT FROM THE CONSUMER'S PERSPECTIVE

Respondents to Aite Group's December 2020 survey reported that their identifying information was used either to create an account that was then used to support monetary theft or to take control of an existing account in order to steal money or loyalty points. Table A breaks out the broad categories of use cases for how criminals make use of identifying information.

Table A: How Identity Thieves Use Fraudulently Acquired PII

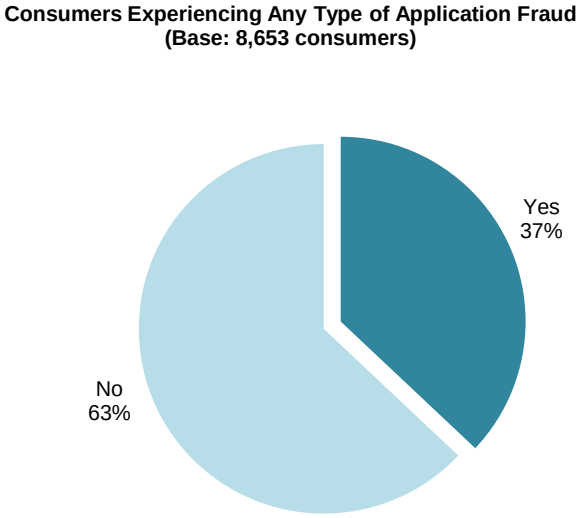
Type of use	Description
Application fraud	Establishing an account that is intended to be used to commission or otherwise support malicious or criminal activity
Account takeover	Obtaining control of an existing account for the purpose of commissioning or otherwise supporting criminal activity

Source: Aite Group

The distribution of these two forms of criminal activity were reported almost equally among those who reported being victimized by identity thieves. Thirty-seven percent of U.S. consumers experienced application fraud in the past two years (Figure 3), and 38% of U.S. consumers experienced an account takeover in the past two years (Figure 4).

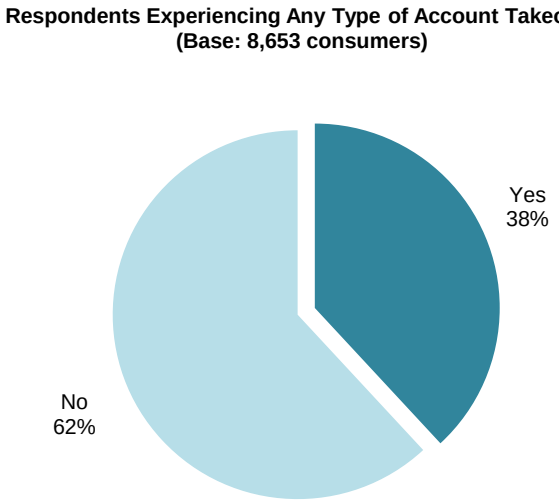
3. "Equifax Data Breach Settlement," Federal Trade Commission, published January 2020, accessed March 8, 2021, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

Figure 3: Application Fraud Victims



Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Figure 4: Account Takeover Victims

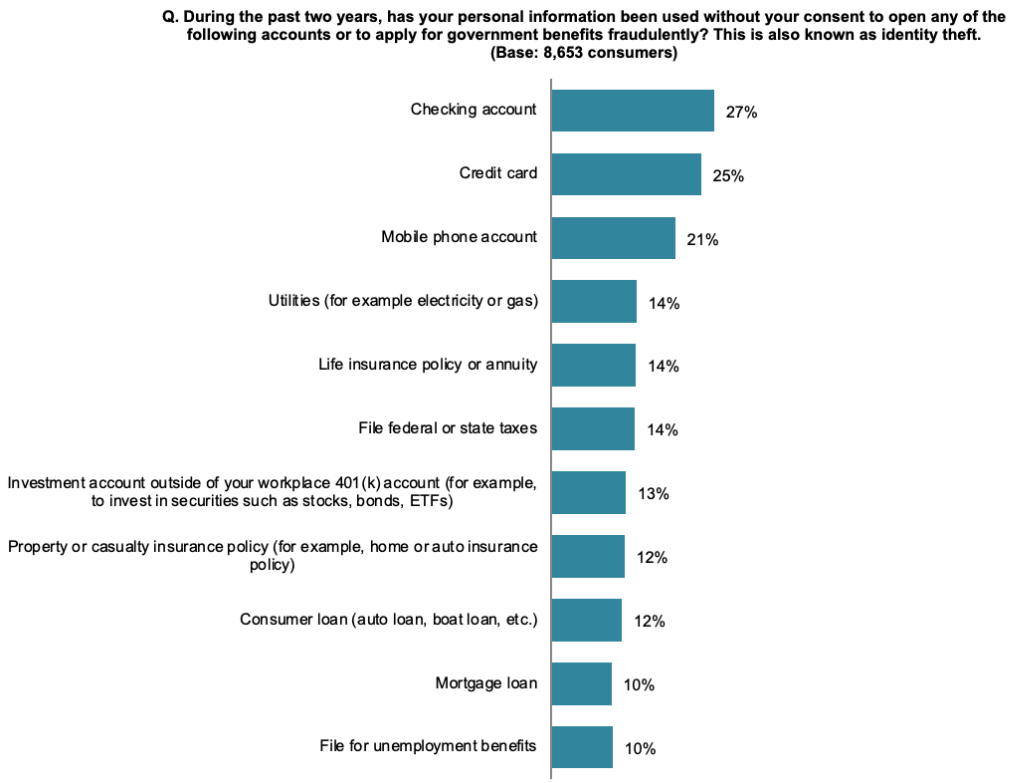


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

While application fraud and account takeover are painfully familiar terms among fraud leaders in the financial services industry, the survey data demonstrate that using fraudulently acquired identifying information for the purpose of creating or controlling accounts is a useful means of thievery regardless of the type of organization that manages the account. While deposit accounts and credit card accounts are the most commonly targeted types of accounts, it's worth noting the wide variety of account types that criminals also commonly target, including mobile

phones (21%), health insurance (17%), utilities (14%), life insurance (14%), property and casualty insurance (12%), and federal and state tax authorities (14%; Figure 5).

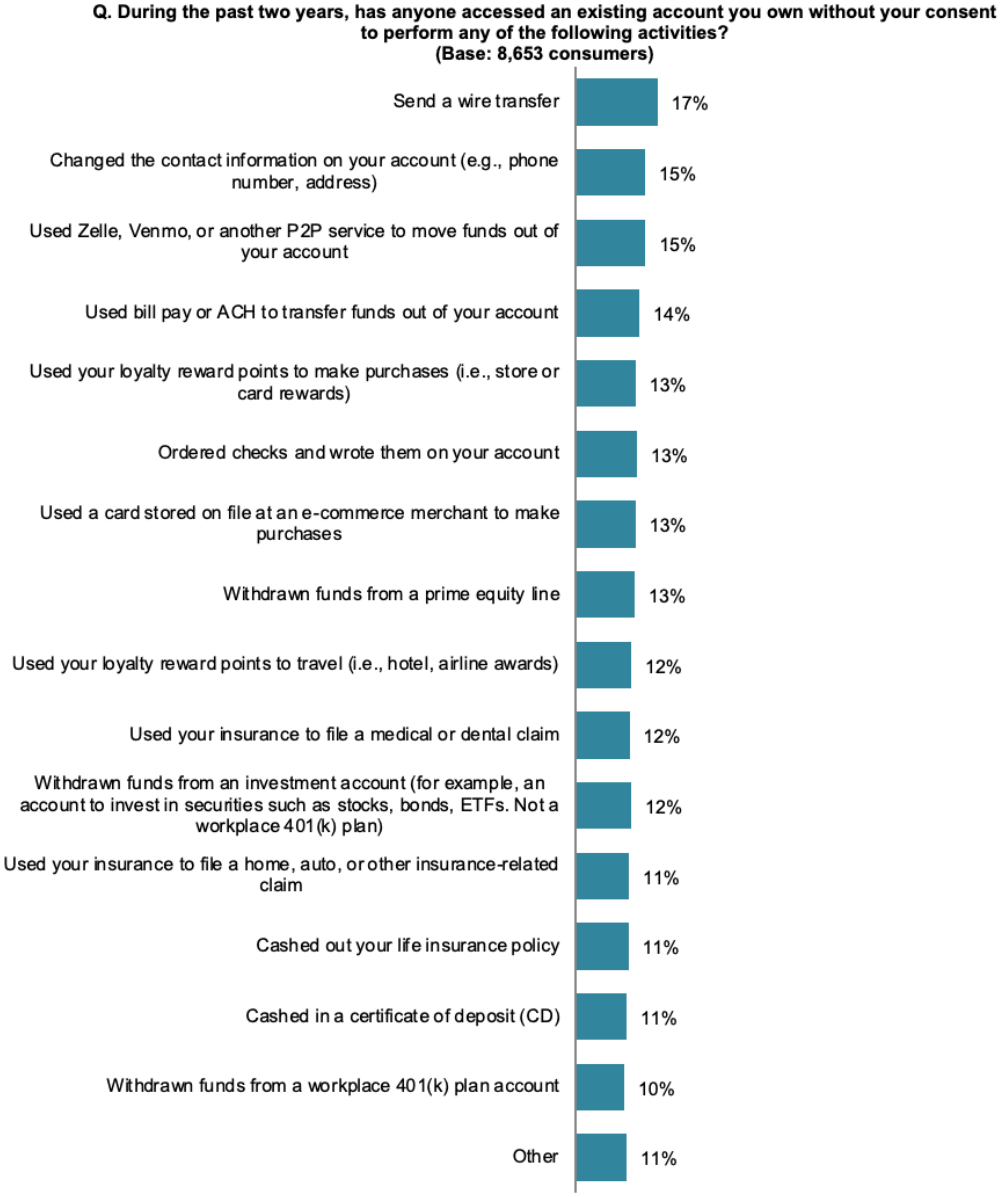
Figure 5: Distribution of the Types of Accounts Created by Fraudsters



Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

While fraudsters also target a variety of accounts for takeover, including card-on-file accounts at merchants (13%), loyalty reward points accounts for making purchases (13%), medical or dental insurance accounts (12%), brokerage accounts (12%), and life insurance (11%) and retirement accounts (10%), wiring funds from bank accounts (17%) was the method of attack that was reported with the greatest frequency (Figure 6).

Figure 6: Distribution of the Types of Criminal Activity Resulting From Account Takeover



Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

The rates of account takeover of loyalty accounts to make purchases (13%) and to pay for travel or accommodations (12%) are both noteworthy and support feedback from fraud executives among financial services providers, merchants, and various travel and hospitality companies who have reported growth in account takeovers targeting loyalty accounts. Many of these fraud executives pointed out that trends among fraudsters to target these accounts have prompted them to increase investments to plug known gaps in their control frameworks. Also noteworthy is that the market forces that govern the kinds of controls that they seek to invest in are the very same forces that influence investment in control solutions engineered to monitor account takeovers in deposit and credit accounts. Regardless of the kind of account they are charged

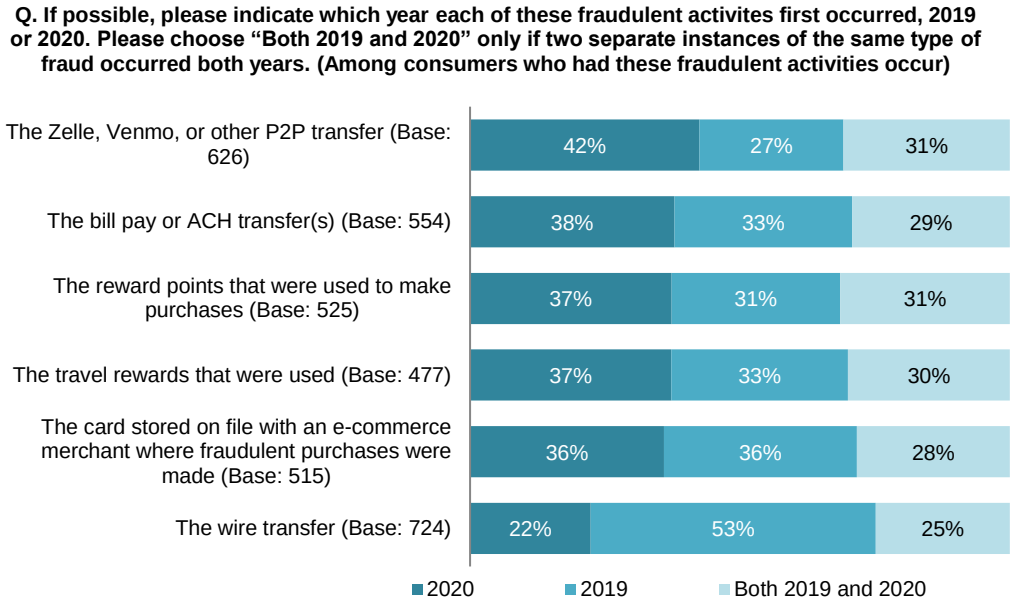
with protecting, fraud executives are under pressure to provide more robust and effective monitoring controls that have either a neutral or positive impact on the client's experience.

TRENDS IN IDENTITY THEFT, ACCOUNT TAKEOVERS, AND APPLICATION FRAUD

While the data from the consumer research revealed a variety of insights into how consumers are impacted by and react to identity theft, the trend that sticks out is the shift in growth patterns that accompanied the pandemic in 2020. At the onset of the pandemic, the conventional wisdom held that fraud losses were likely to increase. This belief followed two commonly held notions among fraud executives. The first is that fraudsters thrive in times of fear, uncertainty, and doubt. The second is that the rate of fraud is inversely correlated with economic prosperity. As the months wore on through the pandemic, however, the patterns of fraud that materialized did not match the expectations of most fraud executives, who held to these notions. Fraud losses did, indeed, increase for many financial institutions, but those losses were not evenly distributed and were considerably milder than most had anticipated.

Respondents from the consumer research reported that account takeover attacks increased for most forms, with the exception of those that resulted in fraudulent wire transfers (Figure 7).

Figure 7: Trends in Types of Account Takeovers Between 2019 and 2020 as Reported by Consumers



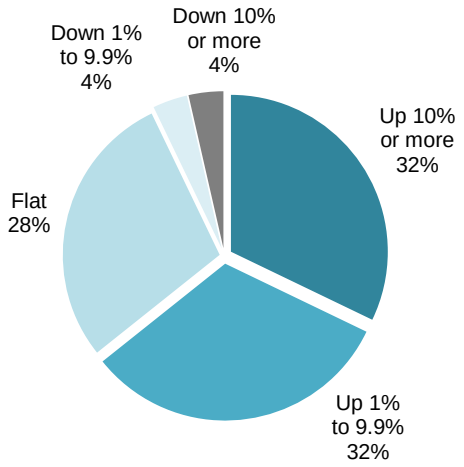
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Overall, the rates of account takeovers reported by consumers are well aligned with account takeover attack rates reported by most financial institutions. The majority of financial

institutions (64%) report that account takeover attacks increased for the same period, with 32% of financial institutions reporting increases of more than 10% (Figure 8).

Figure 8: Rates of Increase in Account Takeover Attacks Reported by Financial Institutions

Q. Please indicate the trend associated with each kind of fraud attack, comparing attack rates today to attack rates prior to the pandemic. (n=28)



Source: Aite Group's survey of 47 financial services fraud executives, September 2020

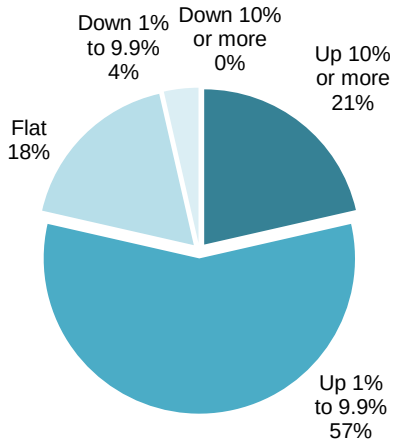
Anecdotally, many of the financial institutions that were among those that reported increases in account takeover attacks pointed out that the majority of their account takeover attacks were concentrated in P2P rails, which aligns well with what consumer respondents report as well.

According to fraud executives, account takeover attacks and application fraud attacks were enjoying steady rates of growth in the years running up to the pandemic.[4] If the environmental conditions surrounding the pandemic gave account takeover attack rates a boost at many financial institutions, then they turbocharged application fraud attacks more broadly across the industry. Figure 9 illustrates that a majority of fraud executives (78%) report increases in application fraud attack rates in 2020, with 21% reporting increases of 10% or more.

4. See Aite Group's report *Application Fraud: Accelerating Attacks and Compelling Investment Opportunities*, November 2020.

Figure 9: Distribution of Application Fraud Attack Rates Reported by Financial Institutions

Q. Please indicate the trend associated with application fraud, comparing attack rates today to attack rates prior to the pandemic. (n=28)



Source: Aite Group's survey of 47 financial services fraud executives, September 2020

The conventional wisdom among many fraud executives holds that the sharp increases in application fraud through 2020 were primarily the result of fraud rings' increased demand for mule accounts. The fraud rings needed the mule accounts to capture and launder funds that were fraudulently intercepted from federal and state unemployment and Small Business Administration loans.

While estimates for losses associated with federal and state stimulus programs are just now beginning to materialize, fraud executives are concerned that the losses are likely to be significant enough to prompt regulators and, perhaps, legislators to increase their scrutiny of how well financial institutions are adhering to existing Know Your Customer (KYC) requirements and to weigh whether more rigorous guidelines are needed. Regardless of the potential fallout from what is likely to be an alarming amount of waste from stimulus programs, virtually everyone agrees that none of the abuse of the financial system's infrastructure would have been possible without a robust market for stolen identities.

CONCLUSION

The market forces that have been driving increases in identity theft, application fraud, and account takeover for years remain very influential, and the environmental conditions brought about by the pandemic have only accelerated those trends. While financial institutions, merchants, and hospitality and travel companies are challenged by these trends, fraud executives and solution providers are countering these threats with solutions that both more effectively manage risk and avoid affecting or even improve the client experience.

- Identity theft, application fraud, and account takeover are not only here to stay but are likely to get worse before they get better.
- Investing in application fraud and account takeover controls remains among the most compelling ways to make substantive improvements to fraud risk, account abuse, and money laundering, and to make significant contributions to growing or optimizing revenue growth.
- Finding the right mix of controls and reducing dependence on those that introduce friction in the important process of acquiring new clients can go a long way toward improving client satisfaction, customer loyalty, and other metrics commonly used to measure client experience, such as net promoter score.
- Behavioral biometrics solutions have enjoyed an increasing amount of investment among financial institutions seeking to deepen their layers of defense against the growing volume of application fraud attacks.

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

Trace Fooshée
+1.857.406.3515
tfooshee@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 ACCERTIFY

Accertify, Inc., a wholly owned subsidiary of American Express, is a leading provider of fraud prevention, digital identity, device intelligence, chargeback management, and payment gateway solutions to customers spanning diverse industries worldwide. Accertify's suite of products and services helps companies grow their business by driving down the total cost of fraud, simplifying business processes, and ultimately increasing revenue.

Accertify Digital Identity is specifically designed to help organizations address the significant rise in fraudulent online account openings and account takeovers. The solution empowers organizations to trust and verify who is on the other side of a digital interaction. Accertify Digital Identity brings together leading machine learning, advanced behavioral analytics, and device intelligence technology to help prevent these sophisticated fraud attacks and keep businesses protected.

CONTACT

For more information, please visit www.accertify.com/adi.