Aite Novarica

JUNE 2022

U.S. IDENTITY THEFT

ADAPTING AND EVOLVING

SHIRLEY INSCOE

This report is provided compliments of:

giact®
A REFINITIV COMPANY

IMPACT REPORT

TABLE OF CONTENTS

IMPACT REPORT

JUNE 2022

U.S. IDENTITY THEFT

ADAPTING AND EVOLVING

SHIRLEY INSCOE

© 2022 Aite-Novarica Group. All rights reserved.

LIST OF FIGURES

© 2022 Aite-Novarica Group. All rights reserved.

© 2022 Aite-Novarica Group. All rights reserved.

SUMMARY AND KEY FINDINGS

Identity theft is a major problem that affects many U.S. consumers each year. This Impact Report focuses on the impact of all forms of identity theft on U.S. individual consumers throughout 2021; it is a follow-up to a report published last year that focused on identity theft in 2020. Using an online survey, 8,520 consumers were asked if in 2021 they had been victims of application fraud or account takeover (ATO)—both forms of identity theft. The key findings from this report follow:

- **Identity theft decreased slightly in 2021:** In 2021, the overall identity theft rate was 25% compared to 27% in 2020. The slight decrease was primarily a result of the ending of many state and federal government subsidy programs related to the COVID-19 pandemic and people who co-habited during the pandemic resuming their normal residences.
- **Forty-six percent of identity theft victims were between the ages of 25 and 44:** Once young adults begin to establish their careers and credit histories, they are more apt to be targeted by identity thieves.
- **Checking accounts, credit card accounts, and mobile phone accounts have the most common forms of application fraud:** Identity thieves open many types of accounts using the personal information of others, but bank accounts are the most common. Fraudsters open mobile accounts so the financial institution (FI) opening the new account can reach the thief (rather than the real consumer).
- **The most common illicit actions performed by a fraudster after an ATO are fraudulent credit card transactions, person-to-person (P2P) transfers, and changing the contact information on the account:** Fraudsters want to steal funds or buy goods quickly, changing contact info so that the FI contacts the thief instead of the legitimate account holder if suspicions arise.
- **Despite identity theft rates declining overall, attacks from unknown parties against consumers aged 55 and older rose sharply from 2020 to 2021:** New digital users, many due to the pandemic, tend to be more naïve and do not protect their personal and confidential data as they should, making them more prone to fall for scams.

© 2022 Aite-Novarica Group. All rights reserved.

- **Consumers in 2021 are significantly less likely to do business with an FI where an account was opened in their name than in 2020:** FIs must have strong application controls or risk incurring a large opportunity cost with application fraud victims.

© 2022 Aite-Novarica Group. All rights reserved.

INTRODUCTION

Identity theft is rampant in the U.S. Consumers become victims when someone uses their personal information to complete an application (e.g., credit or other accounts with financial services firms, government benefits) or when an existing account belonging to them is taken over by an imposter (e.g., an awards account with an airline or hotel, insurance coverage). Consumers need more and better education about protecting themselves from identity theft and some of the scams that involve or can lead to identity theft.

Consumers who are victimized may lose confidence in their provider, may move their business, and likely will make negative comments to family members and friends if they receive poor service as they try to recover from being victimized. Firms that differentiate themselves by providing superior protection and recovery assistance may benefit from a positive reputation and happy customers.

This report examines the rate of identity theft during 2021 and compares it to activity in 2020.[1] The report covers all types of identity theft in financial accounts, insurance, government programs, rewards accounts, etc. It will interest executives in all types of firms and governmental agencies that open or maintain consumer accounts.

METHODOLOGY

GIACT (a Refinitiv company), an industry leader in payments and identity fraud prevention, commissioned Aite-Novarica Group to conduct an online quantifiable survey in the first quarter of 2022. In developing the report, GIACT provided its insight, informed by its understanding and solutions that address today's complex identity theft challenges, to help steer the scope of this report.

Of the 8,520 U.S. consumers aged 18 or older surveyed, 2,133 (25%) experienced some instance of identity theft in 2021. The sampling was click-balanced to the U.S. census for age, gender, income, and region to create an accurate market profile of identity theft. In addition, 3,042 U.S. consumers were surveyed about their familiarity with and experience with criminal scams. The data have a margin of error of approximately 3 points at the 99% confidence level.

1 See Aite-Novarica Group's report U.S. Identity Theft: The Stark Reality, March 2021.

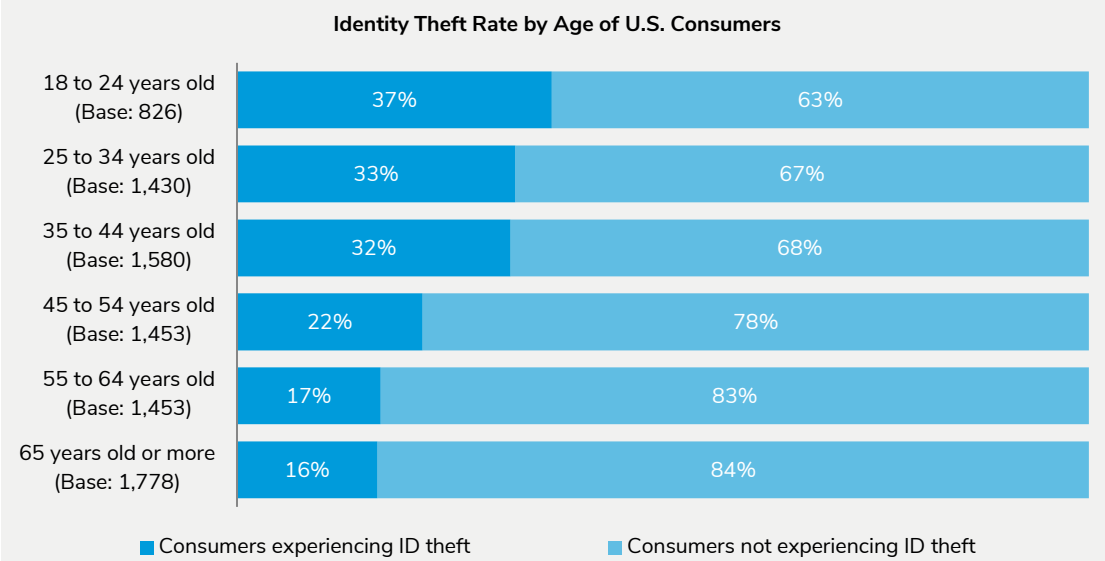
© 2022 Aite-Novarica Group. All rights reserved.

Statistical tests, where shown, were conducted at the 99% level of confidence. Year-over-year comparisons in the report use data from the Q4 2020 survey of 8,653 U.S. consumers aged 18 and older. The 2020 survey was fielded using similar guidelines.

While only minor tweaks were made to question wording, this year's survey included two improvements. First, new definitions and examples of application fraud and ATO fraud were added to ensure clarity and understanding for the survey takers. Second, survey respondents were asked to recollect fraud over a single year rather than two years, which was asked in the 2020 survey. Both of these changes were made to improve data confidence and quality.

No one is exempt from identity theft; all age groups are impacted, as shown in Figure 1. Among younger age groups (consumers aged 18 to 44), the rate of identity theft was much higher than among older age groups (45 and older).

FIGURE 1: AGE OF CONSUMERS SURVEYED AND WHETHER THEY WERE VICTIMIZED

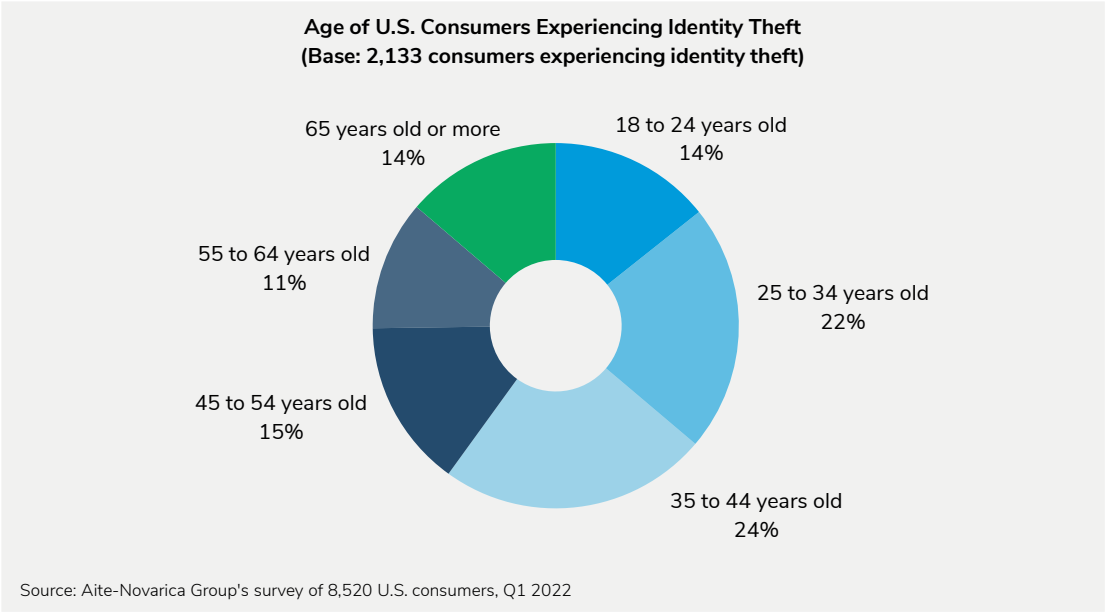


Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

The highest percentage of U.S. consumers (24%) victimized in 2021 were between the ages of 35 and 44 (Figure 2). This group was followed very closely by those between the ages of 25 and 34. Overall, 46% of identity theft victims were between the ages of 25 and 44.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 2: AGE OF IDENTITY THEFT VICTIMS



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

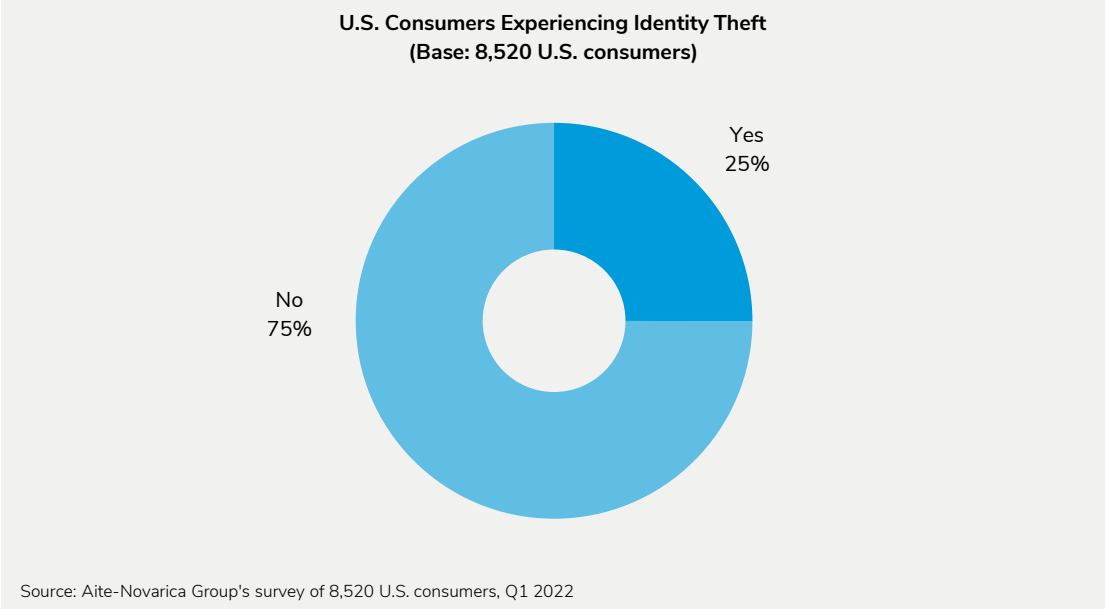
© 2022 Aite-Novarica Group. All rights reserved.

IDENTITY THEFT IN 2021: LET'S TAKE A LOOK

Identity theft continues to plague consumers in the U.S. Identity theft typically occurs in one of two ways: An unauthorized party uses the victim's personal information to apply for a financial account, loan, or some type of benefit (e.g., Medicare), or an existing account or benefit (e.g., medical insurance, rewards for a hotel or airline) owned by the victim is accessed or used by an unauthorized person.

Identity theft soared in 2020. Fraudsters targeted various state and federal government subsidy programs to assist consumers financially during the pandemic, as evidenced in the prior study.[2] Fraudsters fed on these governmental windfalls, stealing many millions of dollars. Identity theft rates fell slightly in 2021 as federal government programs related to the pandemic were phased out, and unemployment programs were scaled back. However, 25% of U.S. consumers, one in every four adults, still experienced identity theft in 2021 (Figure 3).

FIGURE 3: U.S. CONSUMERS EXPERIENCING IDENTITY THEFT IN 2021



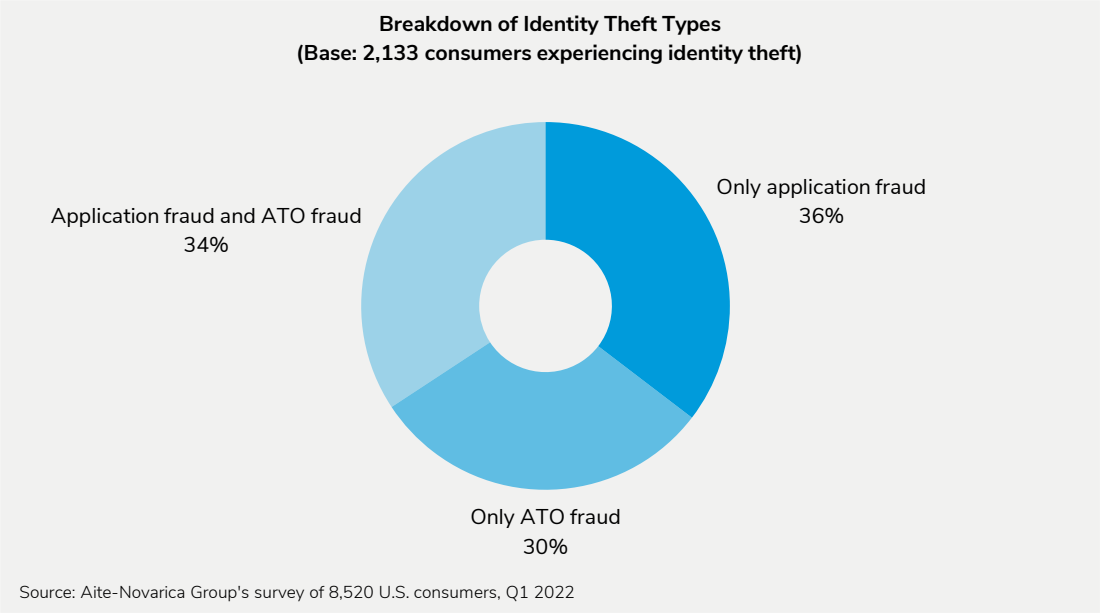
Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

2 See Aite-Novarica Group's report U.S. Identity Theft: The Stark Reality, March 2021.

© 2022 Aite-Novarica Group. All rights reserved.

Among consumers who experienced identity theft in 2021, 34% experienced application fraud and ATO fraud. Thirty-six percent experienced only application fraud, and 30% were ATO victims only (Figure 4).

FIGURE 4: BREAKDOWN OF IDENTITY THEFT EXPERIENCE IN 2021



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

IDENTITY THEFT: 2020 VS. 2021

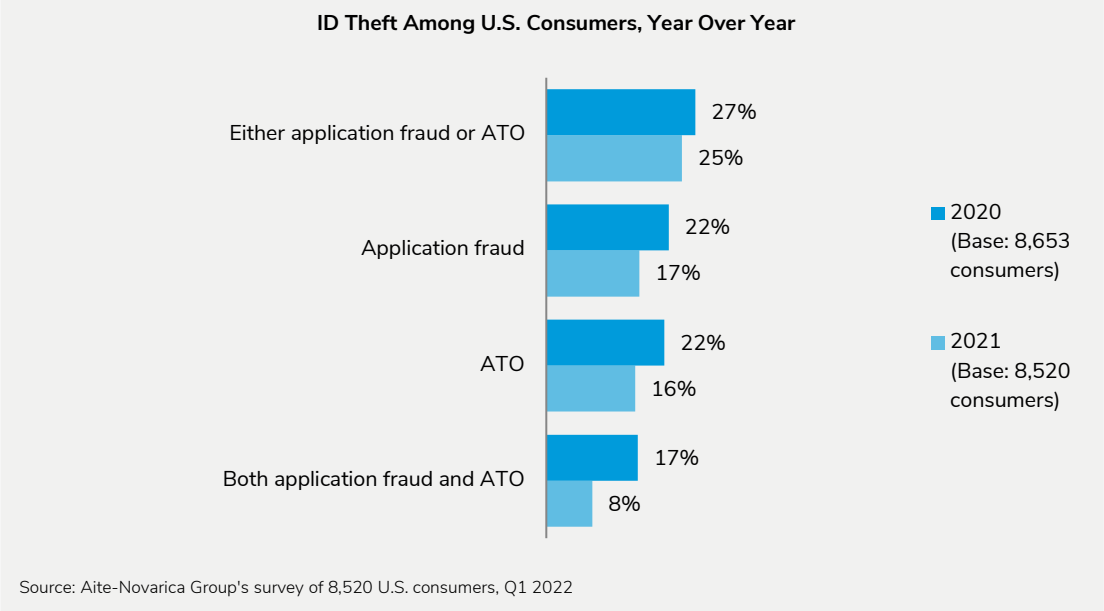
Overall, the percentage of consumers who were victims of identity theft in 2021 fell slightly to 25% from 27% in 2020 (Figure 5). Percentages went down for consumers who experienced application fraud or ATO, as well as those who experienced both types of identity theft.

Many states ended their pandemic unemployment programs, and federal pandemic assistance programs were phased out in 2021. While these programs led to a huge uptick in fraud in 2020, scam activity[3] in 2021 exploded (much of which led to identity theft), causing a much smaller overall percentage decline than otherwise anticipated.

3 See Aite-Novarica Group's report Scams: On the Precipice of the Scampocolypse, March 2022.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 5: IDENTITY THEFT RATE COMPARISON, 2020 AND 2021



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

APPLICATION FRAUD: A DEEP DIVE

Application fraud can occur in many different facets of life. If fraudsters can benefit from stealing money or benefits owned by consumers, they will likely make it happen. In 2021, 17% of consumers were victims of some type of application fraud (Figure 6).

FIGURE 6: CONSUMERS WHO EXPERIENCED APPLICATION FRAUD IN 2021

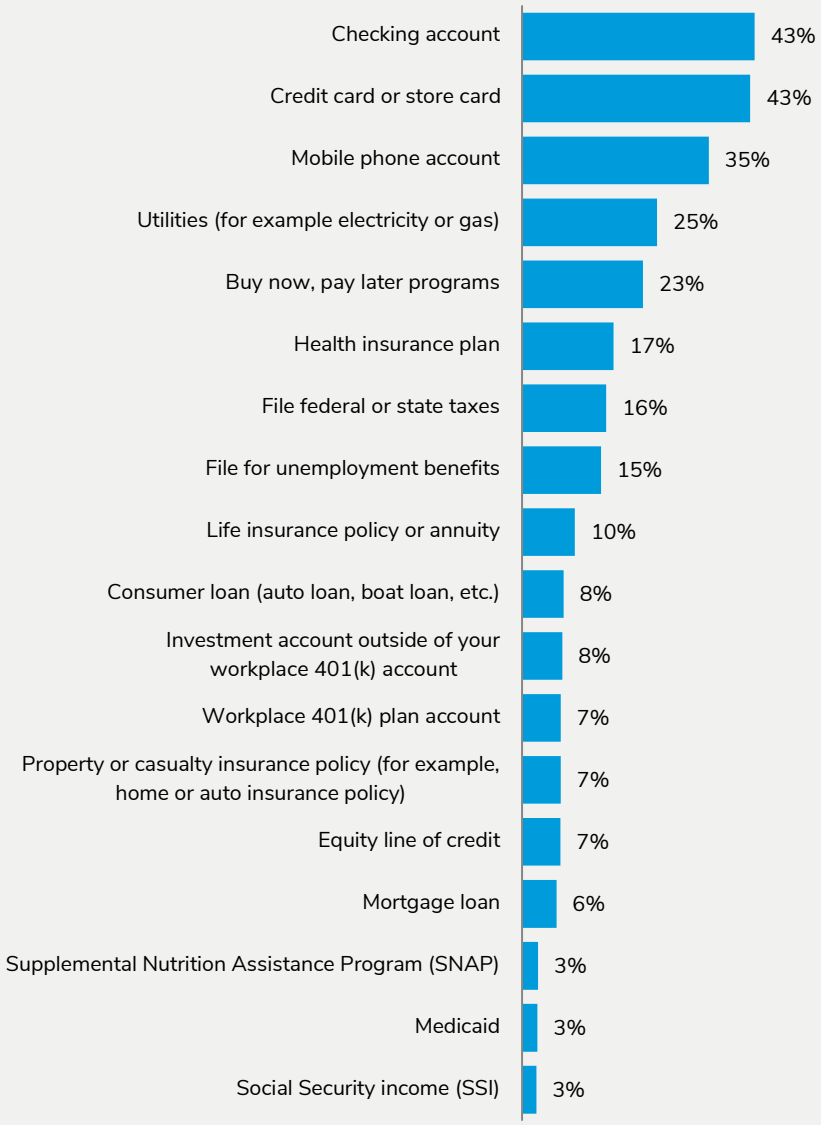
Source: Aite-Nobvarica Group's survey of 8,520 U.S. consumers, Q1 2022

Figure 7 outlines the many ways consumers can fall victim to application fraud. The most common types of application fraud in 2021 related to checking accounts and credit cards (43% each of consumers who experienced application fraud) and mobile phones (35%). Other than filing state or federal taxes (16%) and filing for unemployment benefits (15%), all types of governmental application fraud fell to 3% or less in 2021. These results likely signify that many fraudsters turned their attention away from governmental programs to focus on prior targets such as financial services.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 7: TYPES OF APPLICATION FRAUD EXPERIENCED

Q. During the past year, was your personal information used without your consent to open any of the following accounts or to apply for government benefits fraudulently? (Base: 1,486 U.S. consumers who experienced application fraud)



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

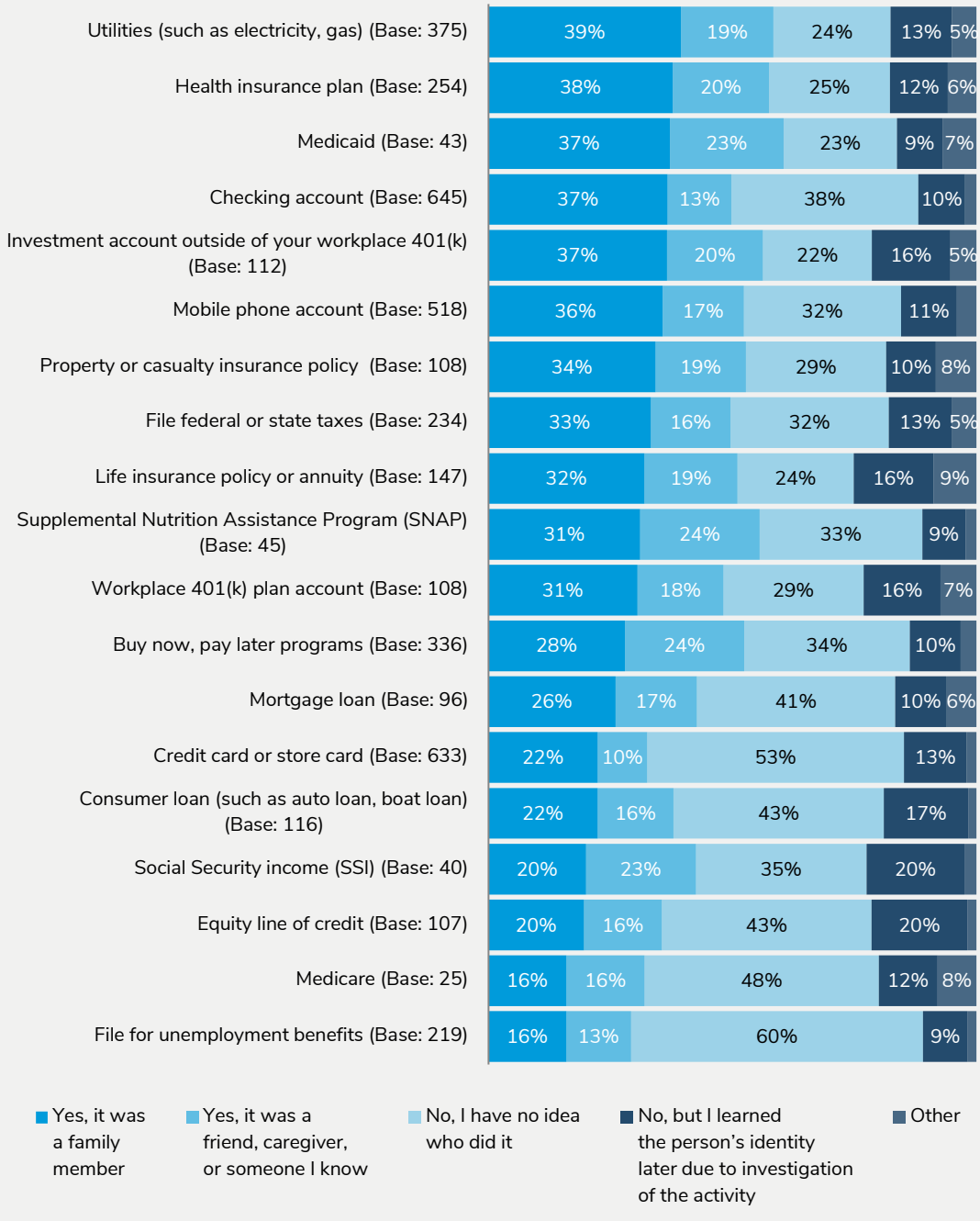
FAMILY AND FRIENDLY APPLICATION FRAUD

Unfortunately, quite a bit of identity theft is committed by family members or friends. These people often have access to a consumer's personal information, so they can successfully complete an application impersonating the consumer. The most common kinds of application fraud committed by friends and family in 2021 include utilities, health insurance, Medicaid, checking account, investment account, mobile phone, property or casualty insurance, and filing state or federal taxes. In all these types of application fraud, at least 33% of victims knew the identity thief (Figure 8).

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 8: FAMILY AND FRIENDLY APPLICATION FRAUD

Q. Did you know the person who used your identity to open the following accounts without your consent? (Among consumers who had these fraudulent accounts being opened)



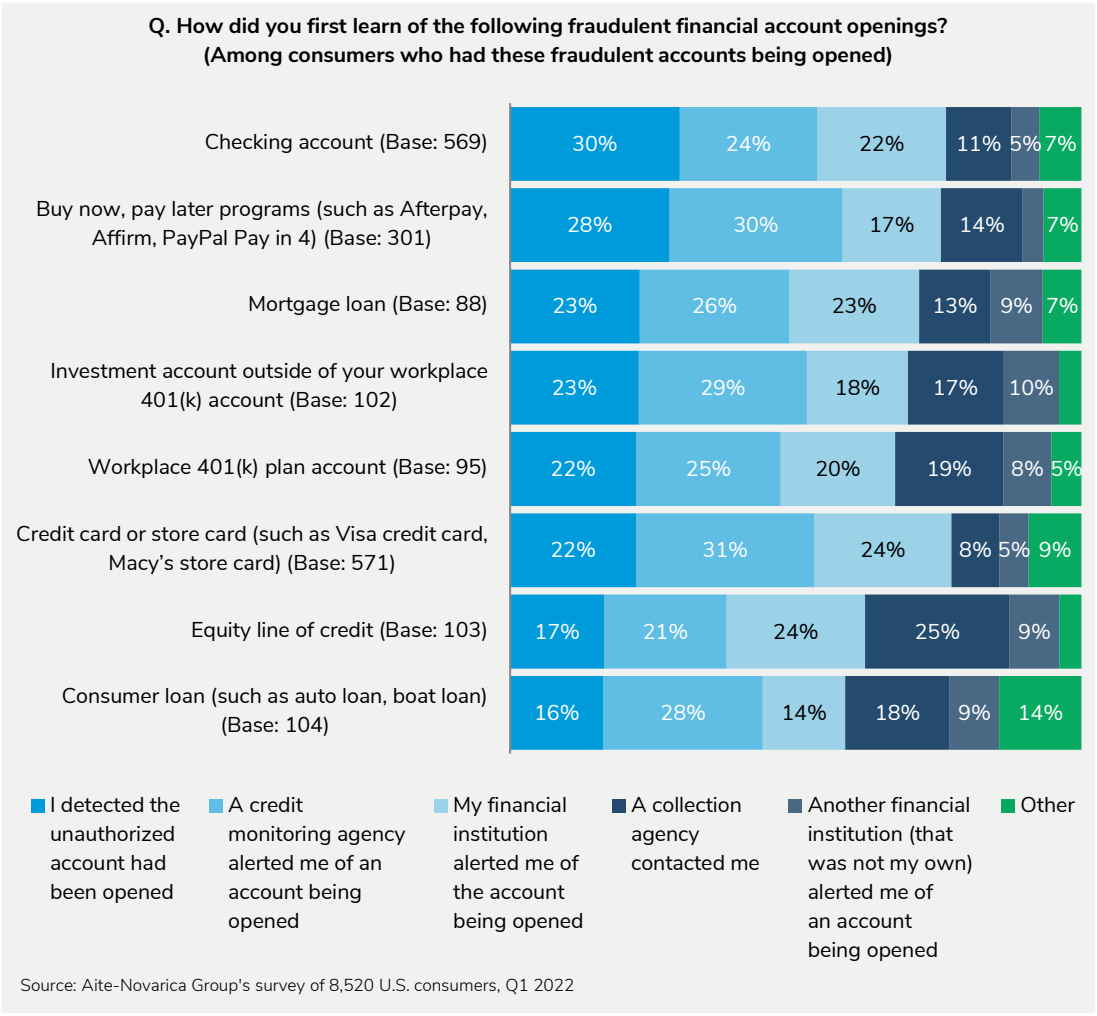
Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

HOW CONSUMERS BECAME AWARE OF APPLICATION FRAUD IDENTITY THEFT

Consumers first learned about having their identities stolen and used to apply for new accounts or benefits in several ways. The three most common ways were detecting the new account or relationship themselves, being alerted by a credit monitoring agency, and being notified by their FI (Figure 9).

FIGURE 9: HOW CONSUMERS BECAME AWARE OF APPLICATION FRAUD



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

Smaller percentages of consumers were alerted by another FI (where a new account was applied for) or a collection agency. Being contacted by a collection agency means the account has been open long enough to be delinquent on payments, and it may be

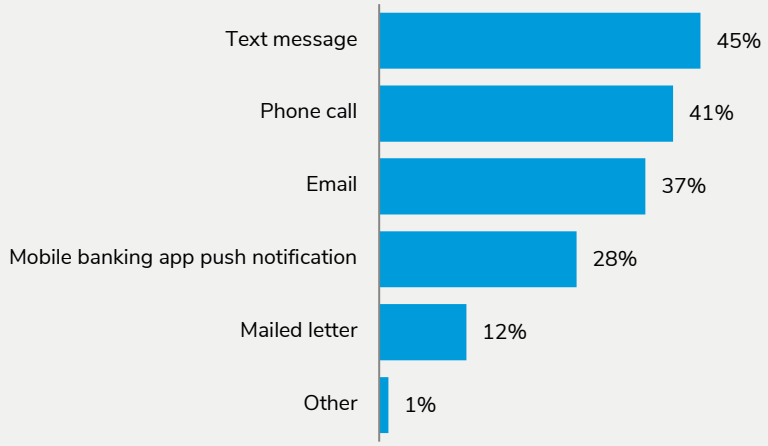
© 2022 Aite-Novarica Group. All rights reserved.

difficult to convince the agency that the account is unauthorized. Often, collectors think the consumer is trying to avoid repaying a debt.

Figure 10 shows how consumers were notified by their FIs that a checking account had been opened in their identity. FIs may use multiple methods of communication in each case when getting a response is difficult or delayed. FIs used similar methods (though percentages differ slightly) to contact consumers when other types of accounts were opened, e.g., credit cards).

FIGURE 10: HOW CONSUMERS WERE NOTIFIED OF FRAUDULENT CHECKING ACCOUNTS

Q. Please select how the financial institution alerted you to the fraudulent checking account opening. (Base: 155 consumers who were first alerted by an FI about this fraudulent activity)



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

Often, FIs will call the "real" consumer when they realize a different address or phone number exists for the person than the one used to open the account. A phone call enables the FI to determine whether the account is legitimate quickly. This method was used in 41% of cases in which the victim of a fraudulent account opening was first alerted by an FI. Text messages and emails can be effective if sent to the actual consumer instead of the identity thief. Push notifications may be more secure than other methods of communication, and mailed letters are less common since they often take several days to deliver.

Buy now, pay later (BNPL) loans are a relatively new method of paying for goods purchased; typically, equal payments are spread over a few short months. Depending on

© 2022 Aite-Novarica Group. All rights reserved.

the type and cost of the good purchased, the pay period may extend several years. This payment type is increasingly falling under regulatory scrutiny[4] due to concerns over credit quality and fear that consumers may acquire more debt than they can handle.

Among consumers who were first alerted by the FIs, email (53%) was overwhelmingly used to contact consumers who were victims of identity theft involving BNPL accounts (Figure 11).

FIGURE 11: HOW CONSUMERS WERE NOTIFIED OF FRAUDULENT BNPL ACTIVITY

Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

Mortgage loans are often the largest loans that consumers obtain during their lifetime. In recent years, mortgage lending has made it very simple for an individual consumer to complete the entire application process online. Unfortunately, this also makes it easier for an identity thief to impersonate the consumer, especially if the thief has access to the consumer's home and can schedule the closing when the consumer is away.

Perhaps because much of the application process is handled online and by email exchanges, email was also the most common method to notify victims of fraudulent

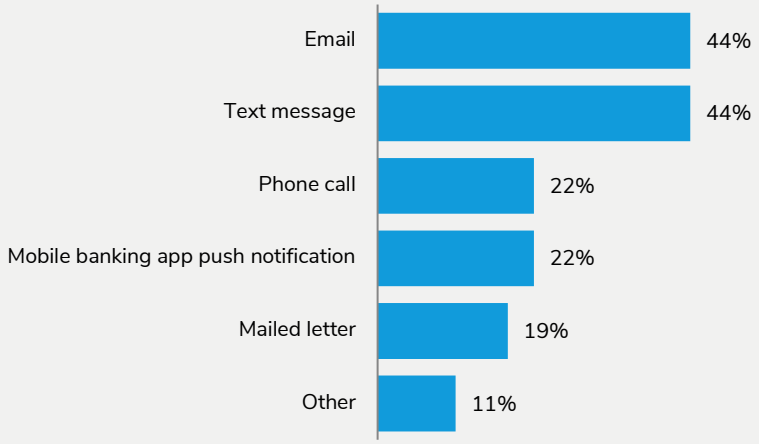
4 Eamonn Moran and Robin Nunn, "CFPB's Probe of Buy Now, Pay Later: What's the Risk to Consumers?," Bloomberg Law, February 15, 2022, accessed April 19, 2022, https://news.bloomberglaw.com/banking-law/cfpbs-probe-of-buy-now-pay-later-whats-the-risk-to-consumers.

© 2022 Aite-Novarica Group. All rights reserved.

mortgage accounts opened in the consumer's name (Figure 12). Forty-four percent of those who were first alerted by an FI stated this is how the FI communicated with them.

FIGURE 12: HOW CONSUMERS WERE NOTIFIED OF FRAUDULENT MORTGAGES

Q. Please select how the financial institution alerted you to the fraudulent mortgage loan account opening. (Base: 27 consumers who were first alerted by an FI about this fraudulent activity)



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

ACTIONS CONSUMERS TOOK UPON LEARNING OF APPLICATION FRAUD

Survey respondents who experienced application fraud were asked what actions they took upon learning of the unauthorized account opened in their name. In the case of checking account application fraud, roughly half (51%) responded that they notified their FI (Figure 13). An additional 31% reported the application fraud to the FI at which the fraudulent account was opened. Nineteen percent reported the activity to law enforcement, and 10% reported it to the Federal Trade Commission (FTC). Ten percent did not report the fraudulent activity.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 13: ACTION TAKEN BY CONSUMERS ON FRAUDULENT CHECKING ACCOUNTS

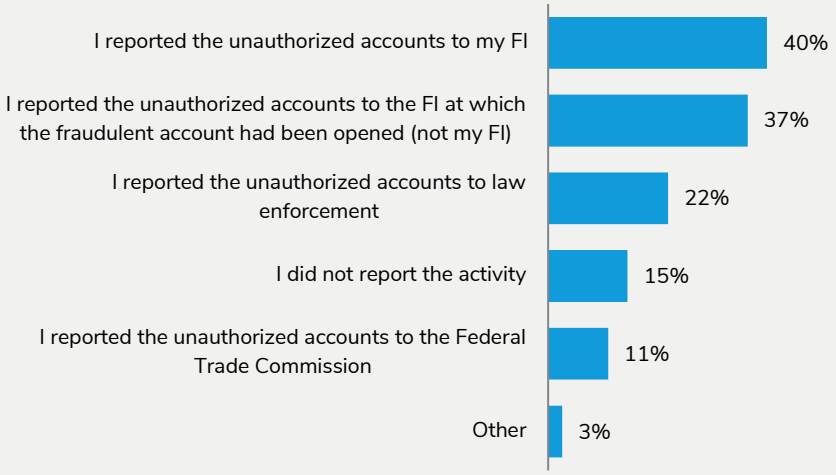
Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

Consumers who were victims of identity theft via new BNPL activity responded somewhat similarly: 40% reported the activity to their FI, and 37% reported it to the FI where the fraudulent activity occurred. Thirty-three percent reported it to law enforcement or the FTC, and 15% took no action (Figure 14). Some consumers may not have even realized what BNPL is.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 14: ACTION TAKEN BY CONSUMERS AFTER LEARNING OF FRAUDULENT BNPL ACTIVITY

Q. When you learned that a BNPL account had been opened without your consent, what did you do next? (Base: 309 consumers who had this fraudulent activity occur)



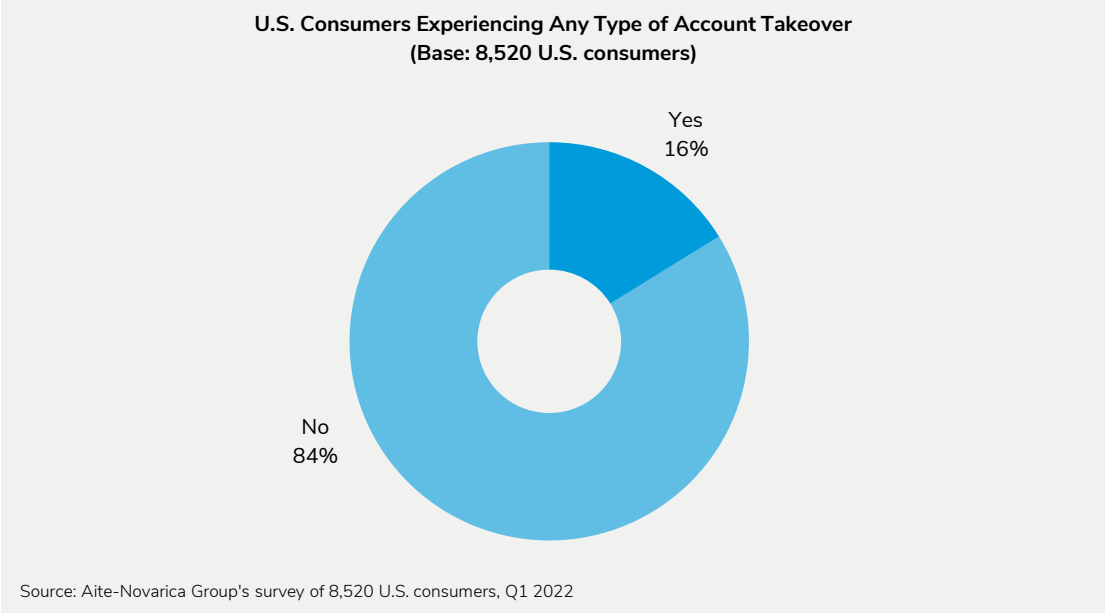
Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

ACCOUNT TAKEOVER: A DEEP DIVE

The other segment of identity fraud consists of existing accounts taken over by impersonators claiming to be the account owner. After taking over the account, the impersonator typically steals funds or other items of value (e.g., travel rewards, insurance benefits) until the true owner realizes that control of the account has been stolen. In 2021, 16% of consumers experienced at least one ATO incident (Figure 15).

FIGURE 15: CONSUMERS WHO EXPERIENCED ATO IN 2021



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

As with application fraud, consumers experienced ATO in different ways:

- The most common type is credit card ATO fraud; 43% of consumers who experienced ATO reported it was of this type (Figure 16). A primary example of credit card ATO involves the unauthorized access to or use of a consumer's card to make fraudulent transactions. Fraudsters can do so by temporarily stealing a card from a consumer or successfully impersonating a consumer and ordering a card through the contact center or other delivery channel. Then, they either watch the

© 2022 Aite-Novarica Group. All rights reserved.

mail to obtain the card before the consumer is aware of it or have the card sent to a different address.[5]

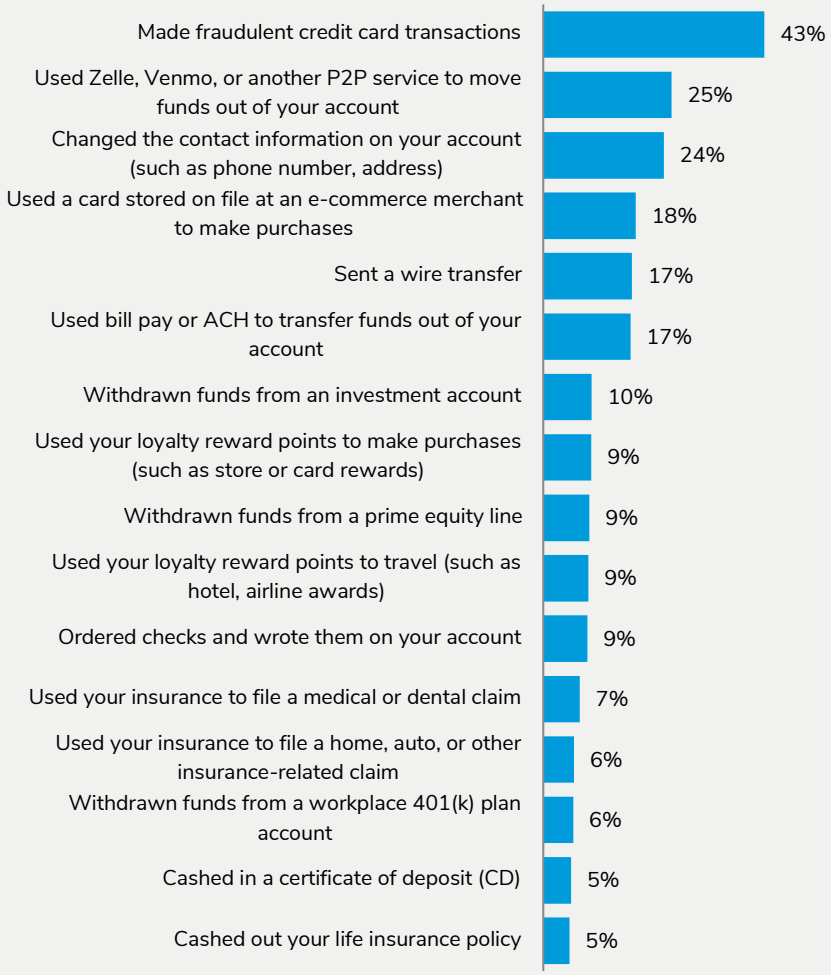
- Twenty-five percent of consumers with ATO fraud experienced a fraudulent P2P transfer to move funds out of an account after an ATO event.
- Twenty-four percent of victims of ATO fraud also had contact information (e.g., phone number, email address) changed after an ATO incident. Fraudsters often change contact information so that if and when the FI reaches out to the consumer to confirm a fraudulent transaction, the contact is made with the fraudster instead of the legitimate account holder so the fraudster can confirm the activity.

5 The distinction between credit card ATO and fraudsters using data obtained through data breaches to perform fraudulent card transactions was carefully explained to survey participants.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 16: ACTIVITY PERFORMED AFTER ATO IN 2021

Q. During 2021, did anyone access an existing account you own without your consent to perform any of the following activities?
(Base: 1,378 U.S. consumers who experienced ATO)



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

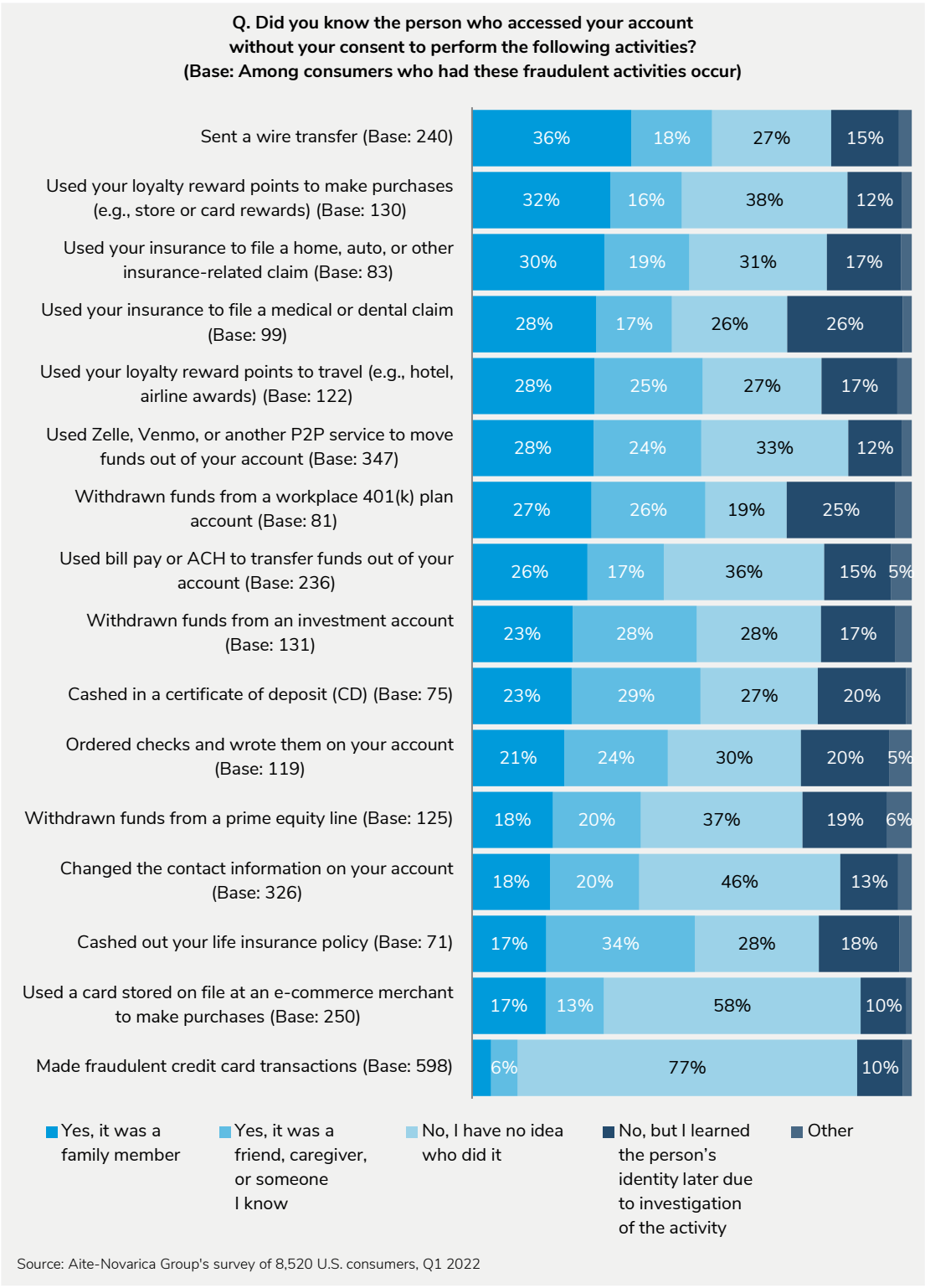
FAMILY AND FRIENDLY ATO FRAUD

Similar to application fraud, family and friendly ATO fraud is performed by those who know the victim (e.g., family, roommates, caretakers) and have access to financial account information, a wallet containing cards, or other information to enable an ATO:

- The most common activity performed by family or friends who commit ATO is to send a wire transfer to move money out of the victim's account (54%; Figure 17). Funds can be moved rapidly to an account the fraudster controls.
- Following wire transfers, friends and family members stole loyalty points for travel or removed funds from a 401(k) account (53% each).
- In 52% of family and friendly ATO fraud instances, thieves used P2P transfers to move funds or cash out a CD owned by the victim. In situations such as this, P2P transfers are attractive because they move money in real time. Thieves don't care whether a CD has matured; the amount of money they steal is reduced slightly by early redemption fees. A consumer who has a CD may not realize it has been redeemed for quite some time if the maturity date is months or years in the future.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 17: FAMILY AND FRIENDLY FRAUD IN ATO FRAUD



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

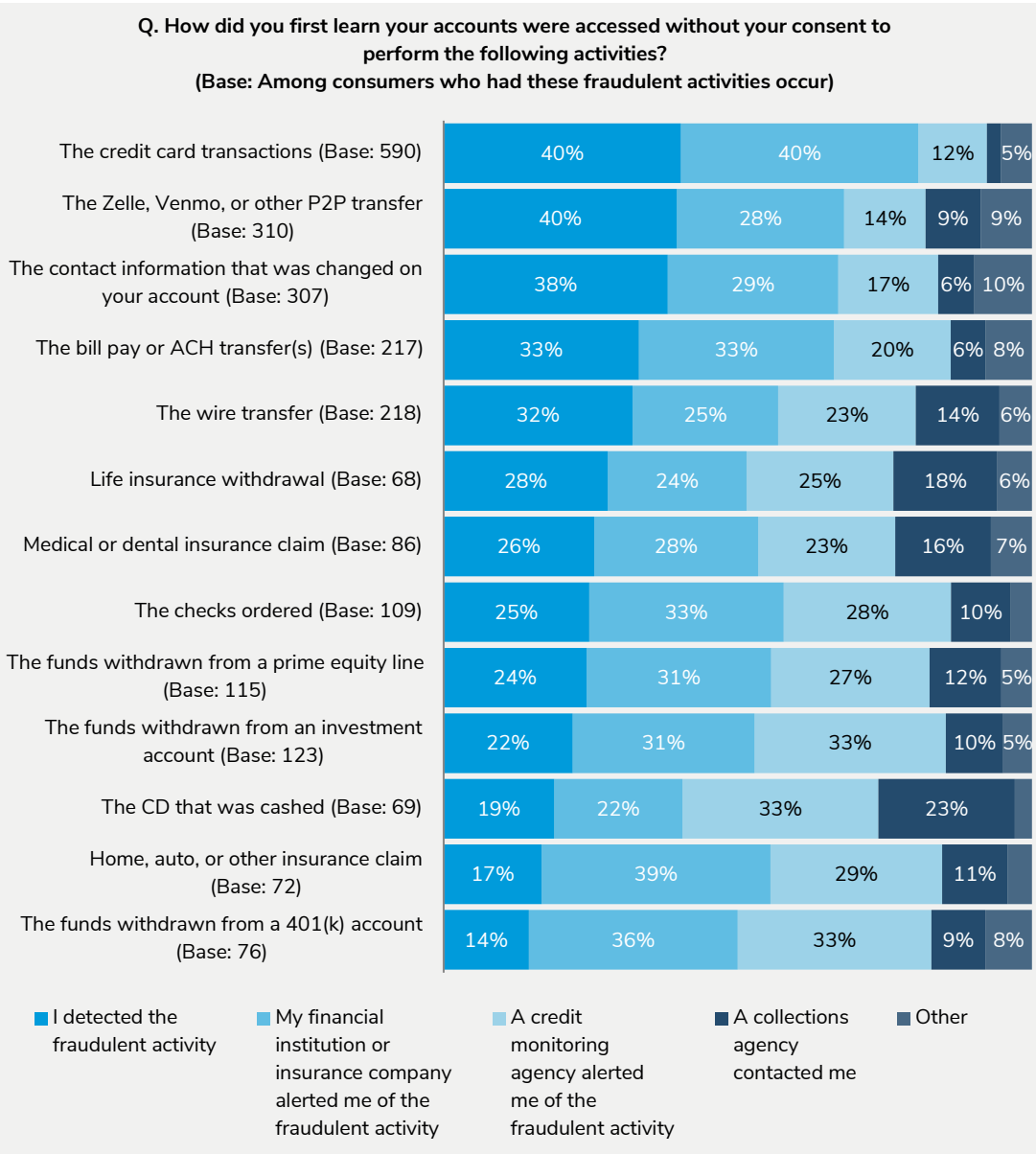
HOW CONSUMERS LEARNED OF ATO INCIDENTS

Victims detect a great deal of ATO activity themselves: reviewing a statement and detecting unfamiliar transactions, seeing an account balance that is lower than expected, receiving mail about activity not performed (e.g., the use of insurance benefits), or seeing a bill for a prime equity line with a higher balance than expected.

Other activities may not be recognized for some time, such as cashing a CD or withdrawing from an investment or 401(k) account. Unless the victim happens to check on these accounts, the theft may not be detected for months. Credit card transactions and bill pay or ACH transactions were detected equally often by the victim and FI. P2P transfers, changes to contact information, wire transfers, and life insurance withdrawals were the other most common victim-detected ATO incidents (Figure 18).

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 18: HOW CONSUMERS LEARNED OF ATO INCIDENTS

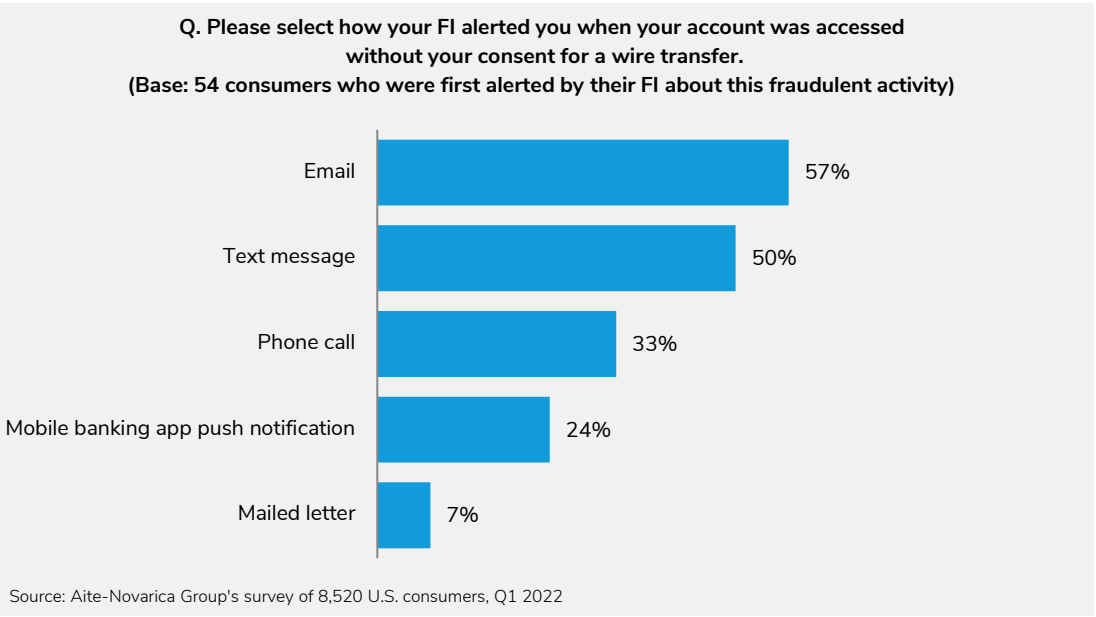


Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

In situations in which the FI was the first to notify the victim of an unlawful wire transfer, it was most often done via email (57%), text (50%), or a phone call (33%; Figure 19). FIs employ multiple ways to contact a consumer because time is of the essence when fraud is involved, particularly with a payment system that moves money quickly.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 19: HOW FIS NOTIFIED CONSUMERS OF WIRE TRANSFERS AFTER ATO



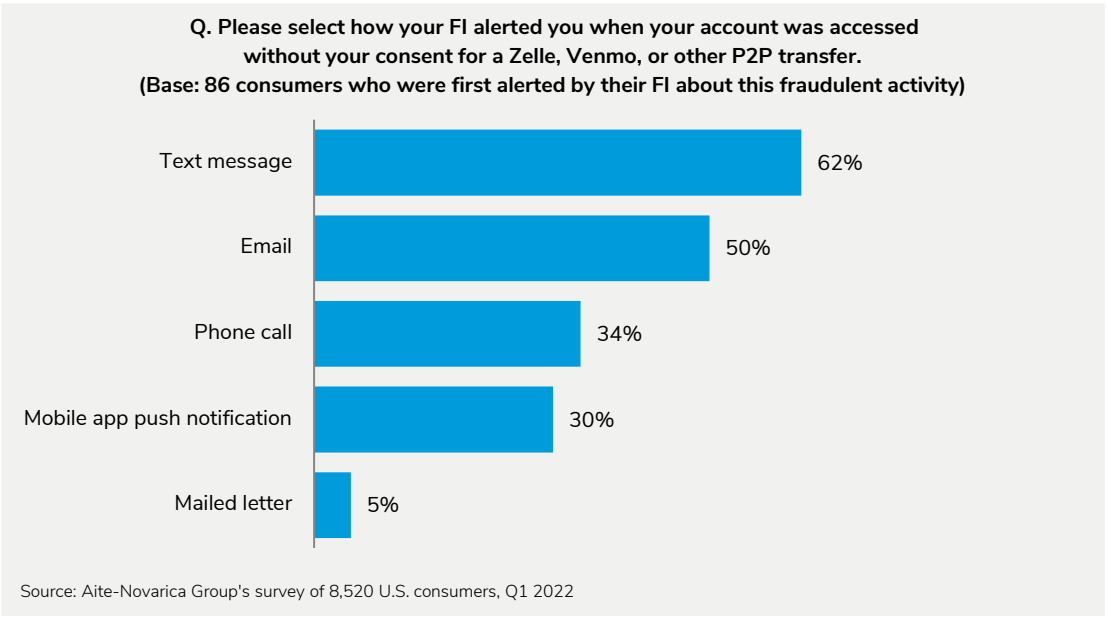
Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

P2P payments are often processed in real time (or near real time); the transfer may be a final payment that cannot be canceled.

In 62% of ATO cases in which customers were first contacted by their FI, the FI contacted them via text message (Figure 20). Fifty percent sent email notifications, 34% called the customer, and 30% notified the customer via a mobile app push message.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 20: HOW FIS NOTIFIED CONSUMERS OF FRAUDULENT P2P TRANSFERS



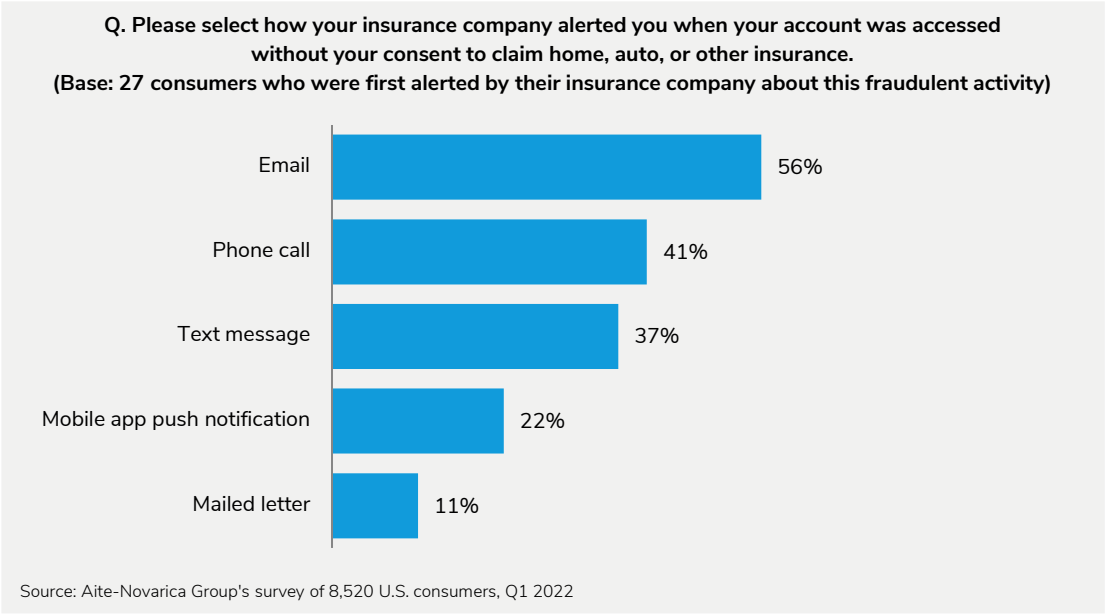
Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

Insurance companies also use various methods to contact their customers when suspicious activity occurs. In cases where property insurance was used, 56% of consumers who were first notified by their insurance company were notified via email, 41% received a phone call, 37% received a text message, and 22% received a push notification via the mobile app (Figure 21).

Eleven percent also received a mailed letter; this could be especially important in the case of family and friendly ATO fraud in which the identity thief is able to intercept electronic communications and keep them from reaching the legitimate customer.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 21: HOW INSURANCE FIRMS NOTIFIED OF FRAUDULENT CLAIMS

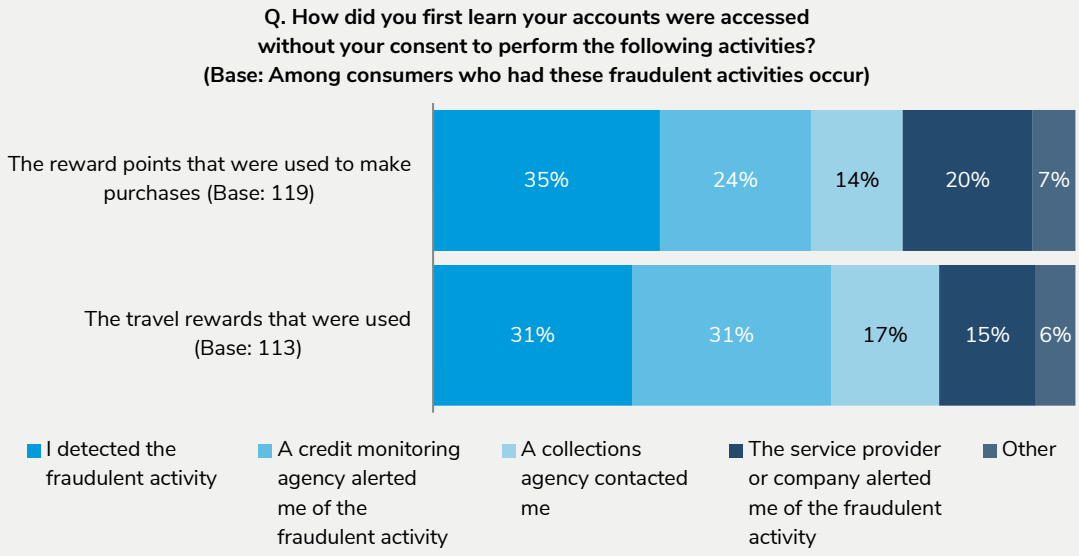


Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

About a third of consumers whose reward accounts were used without their authorization first learned of the theft themselves (Figure 22). If rewards were used to make purchases, the service provider notified the consumer 20% of the time. Only 15% of consumers whose rewards were fraudulently used to make travel arrangements were notified by the service provider. Credit monitoring agencies reported fraudulent activity more often than the service provider offering the rewards account.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 22: HOW CONSUMERS LEARNED OF REWARDS ATO

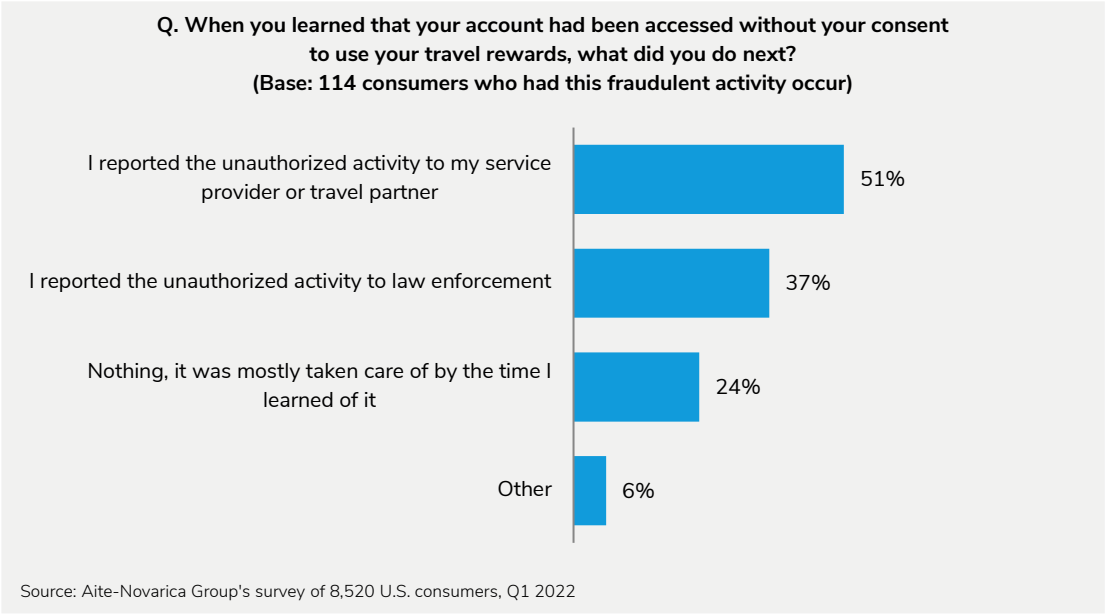


Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

After learning that travel rewards had been used by an identity thief, 51% of victims reported the activity to the service provider offering the rewards (Figure 23). Thirty-seven percent reported the activity to law enforcement. On a positive note, 24% of victims didn't have to do anything because the situation had been resolved by the time they became aware of the theft.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 23: ACTION TAKEN AFTER LEARNING OF REWARDS ATO INCIDENT

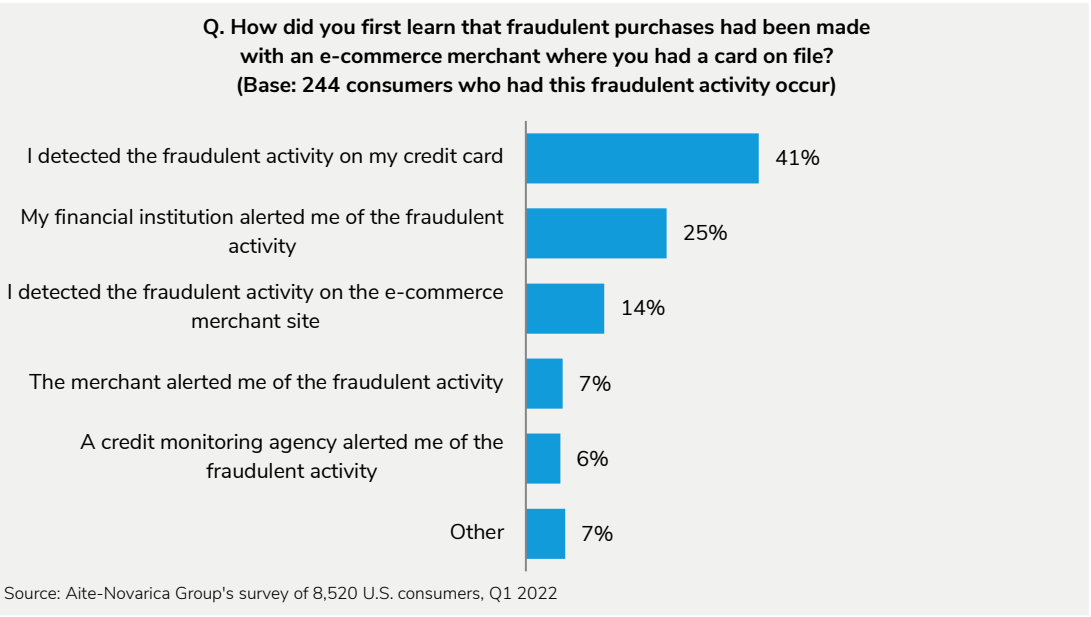


Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

Among consumers who had fraudulent purchases made with an e-commerce merchant with which they had a card on file, 55% detected the ATO themselves by reviewing their credit card activity or reviewing activity on the merchant's website (Figure 24). Twenty-five percent were first made aware of the fraud by their FI; only 7% were made aware of the fraud by the merchant storing the card information.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 24: HOW CONSUMERS LEARNED OF E-COMMERCE ATO INCIDENTS



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

After learning of the ATO with the merchant where a card was on file, 64% of victims reported the fraudulent activity to their FI (Figure 25). Thirty-eight percent reported the fraud to the merchant where the card was on file, and 10% reported it to the FTC. Twelve percent didn't have to do anything because the fraud was resolved by the time they learned about it.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 25: ACTION TAKEN AFTER LEARNING OF E-COMMERCE ATO INCIDENT

Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

CONSUMER SATISFACTION AFTER ATO

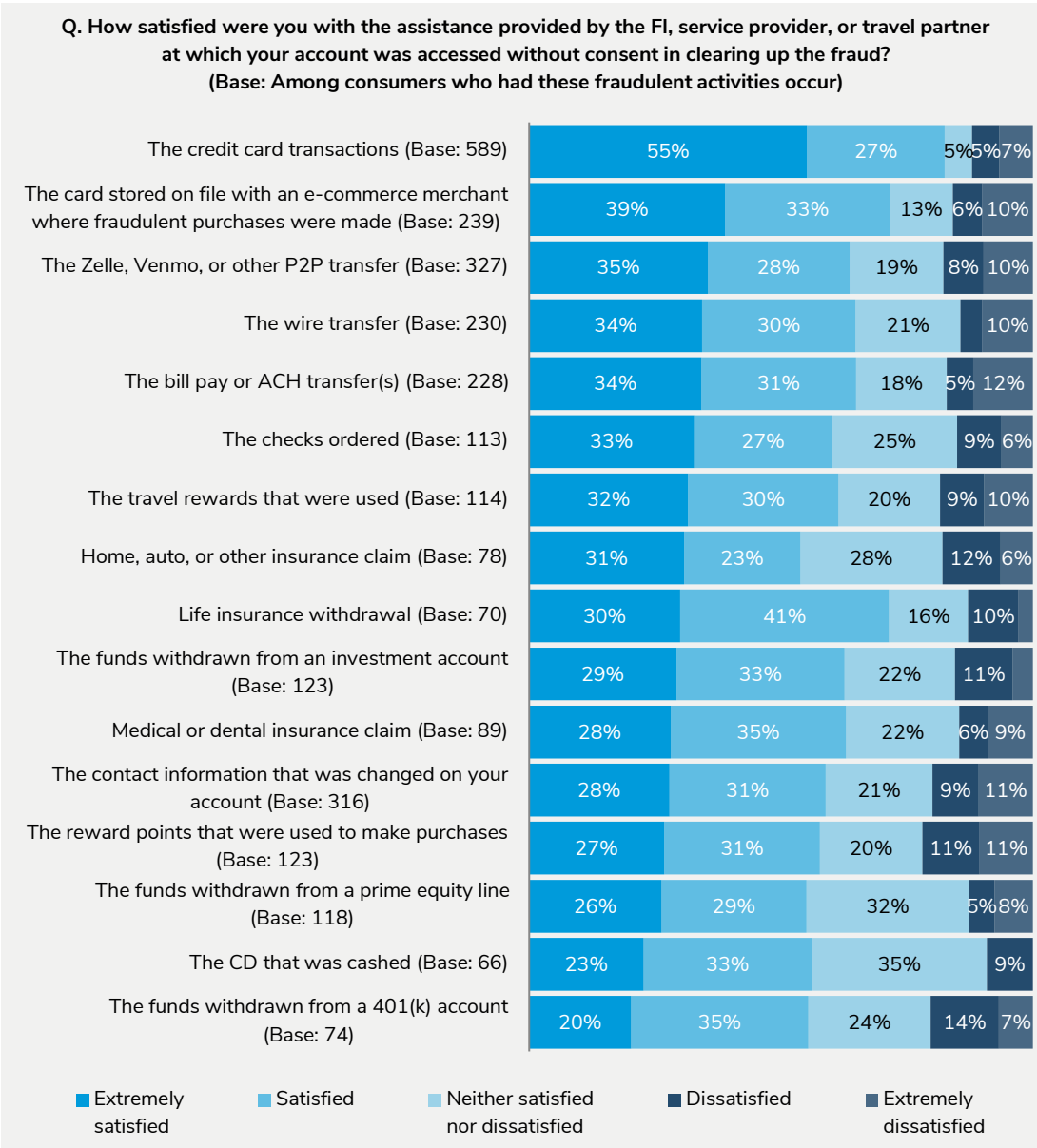
Consumers react differently after an ATO experience. Their level of satisfaction can vary depending on how the fraud is resolved, how they are treated during the process, how long it takes to resolve the incident, and many other factors:

- Credit card fraud occurs often enough that most issuers have well-honed processes to assist customers after the event. These processes work so well that 82% of consumers who experienced a credit card ATO were satisfied with how their situation was handled.
- The second highest category of satisfied consumers after an ATO incident were consumers who had a card on file with a merchant used fraudulently (72%).
- The third highest category of satisfaction was those with a life insurance withdrawal made (71%; Figure 26).
- Categories with the highest rate of dissatisfaction included rewards used to make purchases (22%), funds withdrawn from a 401(k) account (21%), and contact information changed on an account (20%).

© 2022 Aite-Novarica Group. All rights reserved.

All firms should examine their processes to ensure they emphasize customer service to employees handling ATO cases and show respect to all consumers. Firms with understaffing issues will lose the business of some of these consumers if their cases are not resolved in a reasonable amount of time.

FIGURE 26: SATISFACTION LEVEL WITH PROVIDER AFTER AN ATO INCIDENT



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

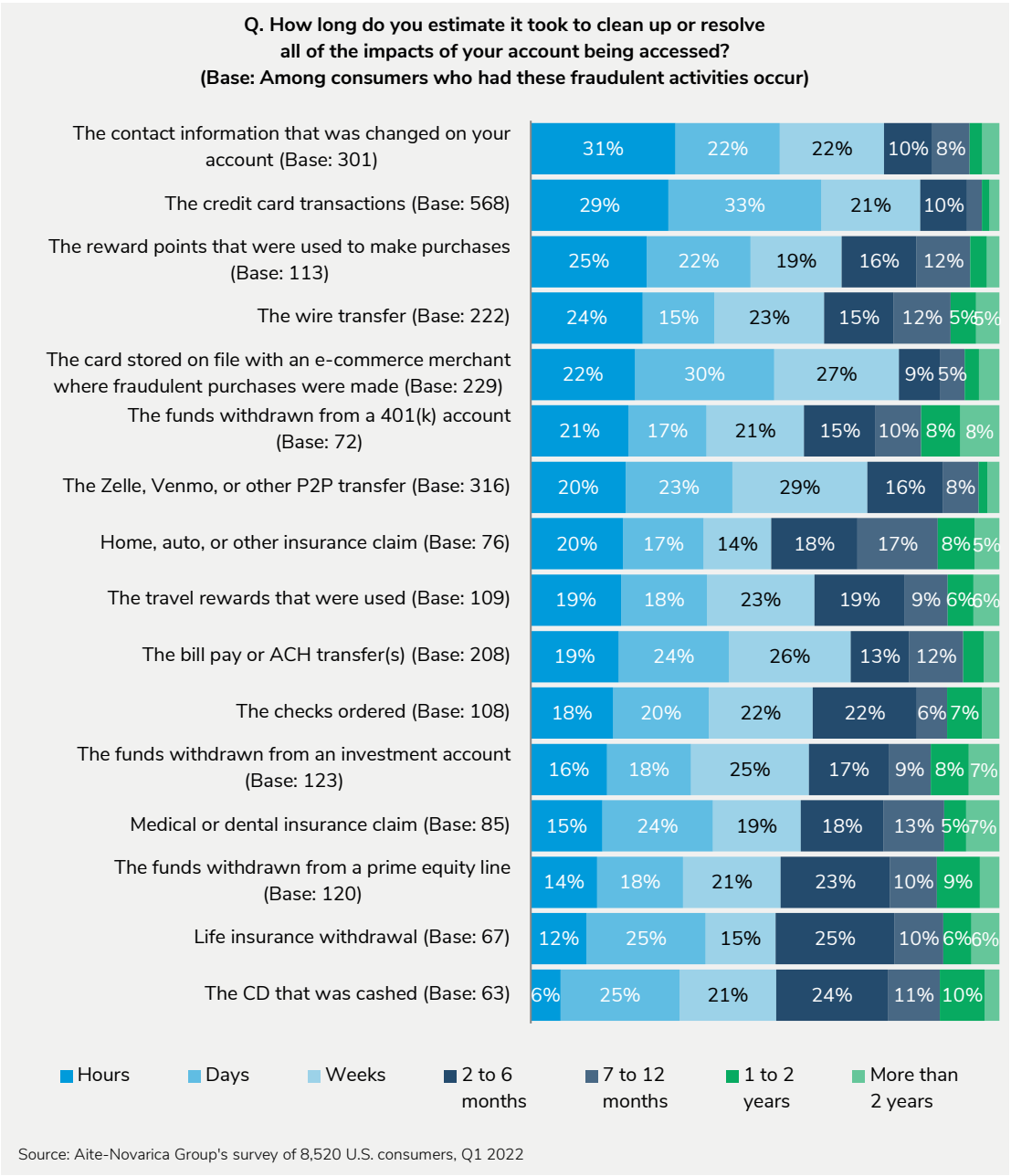
TIME REQUIRED TO RESOLVE ATO

Some identity theft cases are open far too long, leaving many victimized consumers frustrated and compelled to take their business elsewhere. It should be possible to resolve most identity theft cases in a few weeks or a few months at most. Most cases are resolved fairly quickly, but some remain unresolved after more than two years.

In this sample of 8,520 consumers, over 220 ATO incidents took over a year to resolve. Types of ATO cases in which at least 10% of consumers had open cases after a year or more include wire transfers, 401(k) account withdrawals, property insurance claims, used travel rewards, ordered checks, withdrawn investment account funds, medical or dental insurance claims, withdrawn prime equity account funds, life insurance withdrawals, and cashed out CDs (Figure 27).

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 27: LENGTH OF TIME REQUIRED TO RESOLVE AN ATO INCIDENT



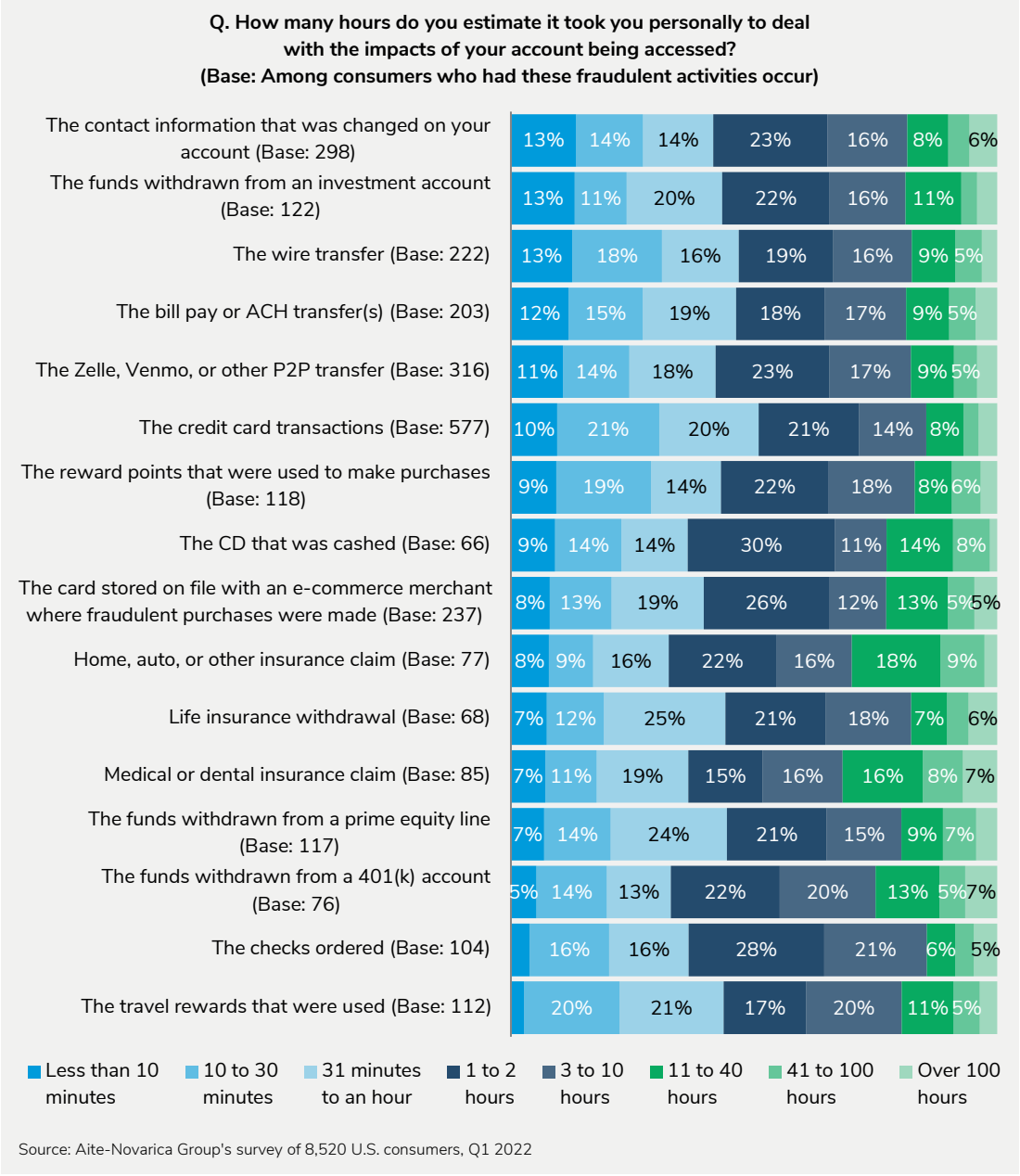
Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

The time consumers have to spend to resolve an ATO incident also varies significantly. The good news is that many consumers resolve the incident in minutes or hours. The bad news is that far too many consumers spend over 100 hours trying to resolve their ATO incidents.

© 2022 Aite-Novarica Group. All rights reserved.

In this survey, 120 ATO incidents required victims to spend over 100 hours resolving them (Figure 28). In some cases, the victims are victimized by identity thieves again by the time they finally resolve the incident.

FIGURE 28: HOURS CONSUMERS SPENT RESOLVING ATO INCIDENTS



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

EASE OR DIFFICULTY OF THE INVESTIGATIVE PROCESS

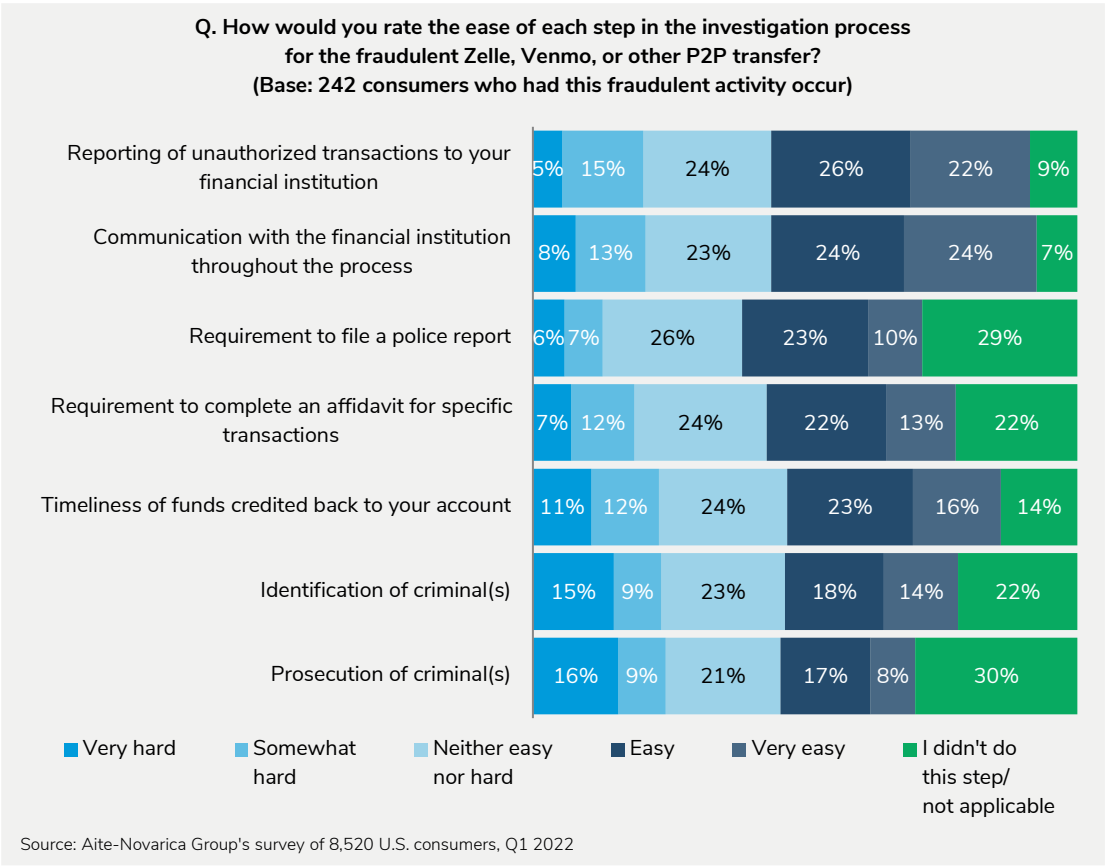
There are many facets to an ATO investigation; several questions need to be resolved. Does the victim know the perpetrator? Did the victim benefit from the activity the victim is reporting? Is the victim willing to prosecute the friend or family member involved? Did the customer actually perform the disputed transactions? The list goes on and on.

Some cases are cut and dry, while others require extensive interviews and other investigative work. Victims often claim they are treated like criminals, but the unfortunate fact is that too many reported fraud incidents are performed by true customers who later dispute the legitimate transactions they performed.

As shown in Figure 29, responses are all over the board concerning P2P transfers. This is generally consistent with consumers' perceptions of the investigative process for other ATO incidents. Managing consumer expectations is also part of an investigator's responsibility. Be honest about what is achievable; for example, many consumers who have funds stolen from their account have a strong desire to see the criminal caught and prosecuted. If there are no known suspects, the investigator has to break the news that this is unlikely to happen.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 29: EASE OR DIFFICULTY OF THE INVESTIGATIVE PROCESS



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

IMPACT OF ATO ON CUSTOMER CONFIDENCE IN FIS

In 2021, 1,032 consumers (out of 8,520 surveyed) experienced one or more ATO incidents on accounts at an FI. These consumers were asked to react to various statements concerning the impact of the ATO experience.

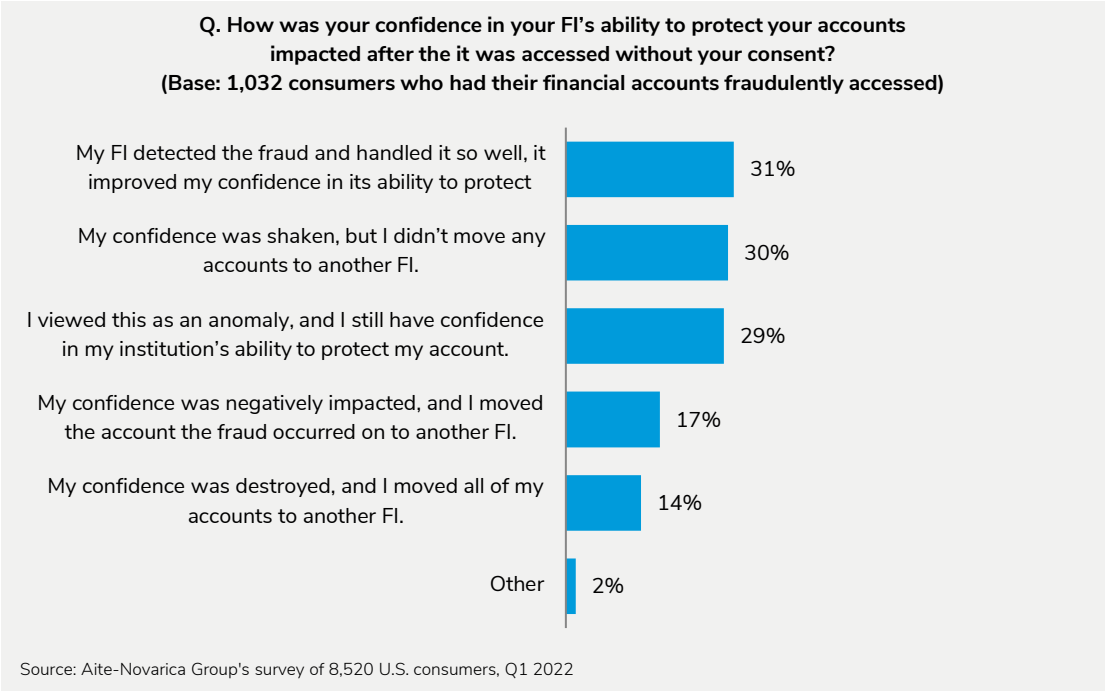
Fourteen percent[6] stated their confidence in their FIs' ability to protect their account was destroyed, and they moved their entire relationship (Figure 30). An additional segment of consumers stated their confidence was negatively affected, and they moved the account that the identity thief took over. Almost a third of consumers said their confidence was shaken, but they did not move any accounts.

6 This chart does not add to 100% because some consumers had more than one ATO incident in 2021 and responded differently to this question depending on what type of account was impacted and the resultant experience.

© 2022 Aite-Novarica Group. All rights reserved.

On a positive note, many consumers said they either viewed the incident as an anomaly or their FI handled it so well that they still have confidence in the FI. To retain customers after an ATO incident, FIs must detect the fraud (if possible) before the customer does, take corrective action as quickly as is feasible, communicate well with the customer throughout the investigation, and listen to the customer throughout the process, responding to their questions and concerns.

FIGURE 30: IMPACT OF ATO ON CONFIDENCE THE CONSUMER HAS IN FI PROTECTION



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

IDENTITY THEFT: 2020 VS. 2021

Several factors led to the slight decrease in identity theft in 2021 compared to 2020: the end of government subsidy programs, people who cohabitated during the pandemic moving back apart, and some firms adopting sophisticated fraud prevention methods. It is important to take a closer look into some of the key differences between 2021 and 2022, as identity thieves will not give up, and the methods of many scam artists will continue to evolve, resulting in more people falling for their scams and schemes.

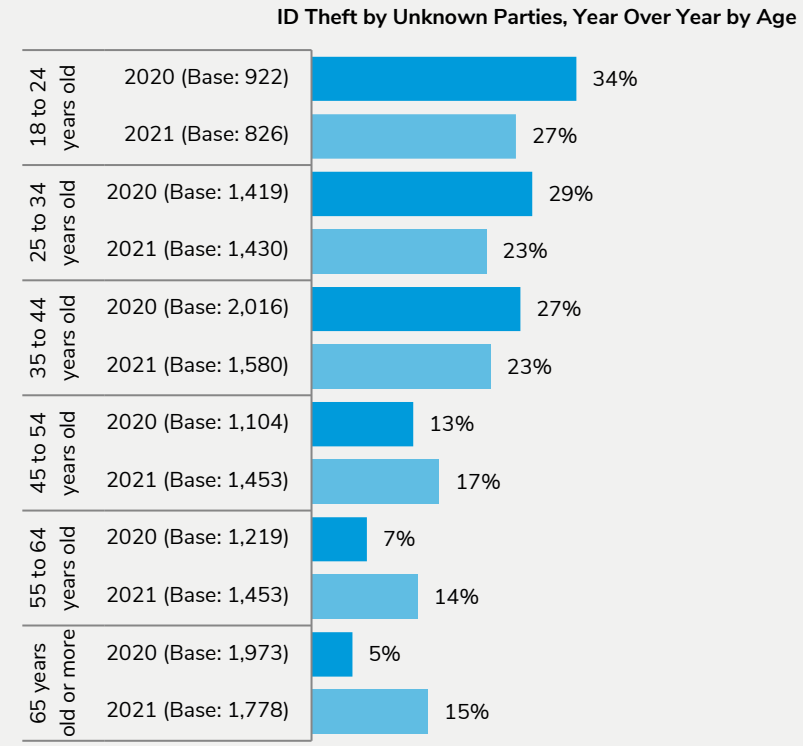
DIGITAL CHANNEL NEWBIES

During the early months of the pandemic, millions of consumers were forced to use digital channels for the first time due to the closures of FI branches, retail stores, and other types of firms. These consumers, often referred to as digital newbies, are typically less apt to recognize a scam than those who have been active online far longer.

Identity theft decreased overall in 2021 compared to 2020, but consumers over the age of 55 were victimized at significantly higher rates in 2021 than in 2020 (Figure 31). Digital newbies need much more education about protecting themselves and their accounts and spotting potential scams when using online and mobile delivery channels.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 31: ID THEFT COMMITTED BY UNKNOWN PARTIES



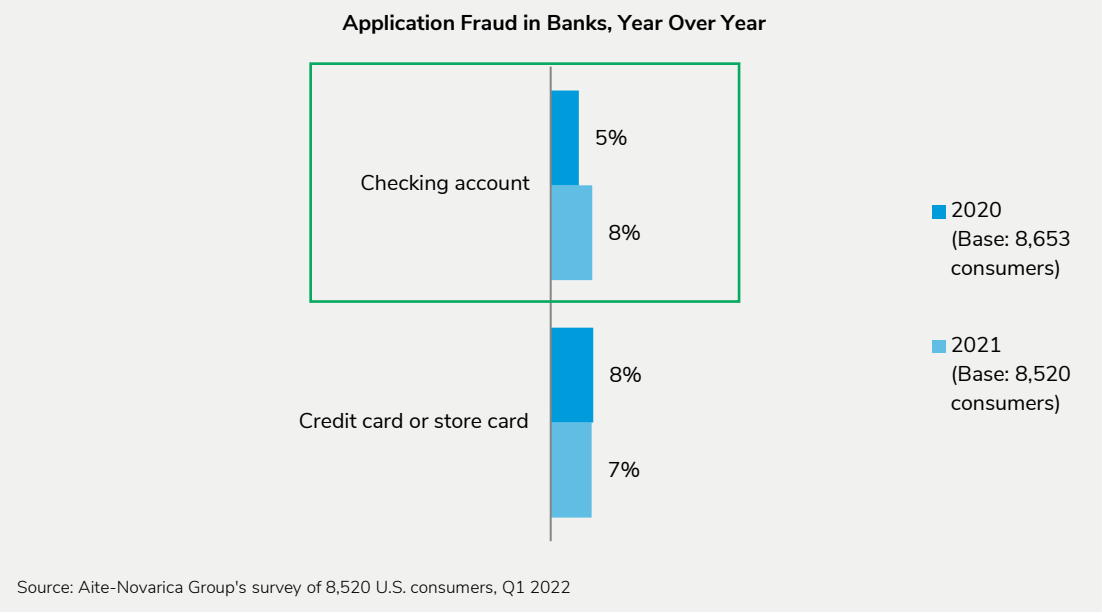
Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

INCREASE IN CHECKING ACCOUNT APPLICATION FRAUD

Several types of application fraud decreased from 2020 to 2021, but there was a significant increase in checking account application fraud: 8% in 2021 compared to 5% in 2020. Credit card application identity theft rates remained similar (Figure 32).

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 32: YEAR-OVER-YEAR APPLICATION FRAUD COMPARISONS



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

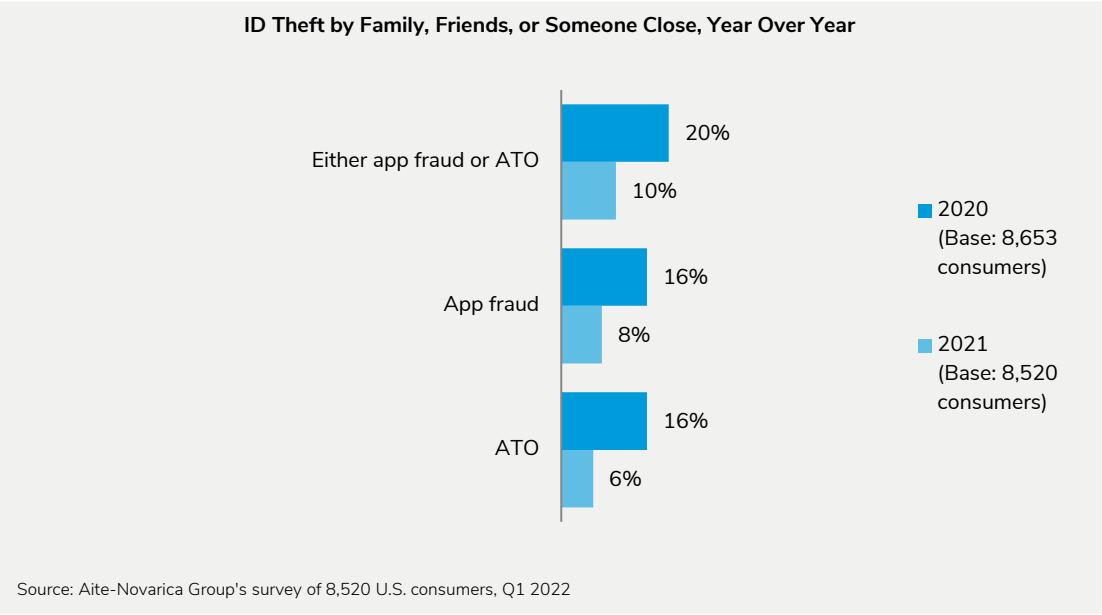
FAMILY AND FRIENDLY FRAUD

Identity theft committed by family members and friends decreased across the board in 2021 compared to 2020 (Figure 33). Family and friendly fraud accounted for 20% of total identity theft in 2020 but only 10% in 2021. In 2020, 16% of application fraud and ATO activity was committed by friends and family. In 2021, only 8% and 6%, respectively, were committed by people known to the victim.

Many people moved in with others during the pandemic. College students moved into apartments together when universities closed dormitories. Many young adults moved back in with parents or grandparents during the pandemic. Families left cities to live with friends in the suburbs or rural areas. Most of these people are no longer living as they were during the worst months of the pandemic, and identity theft committed by friends or family members has fallen accordingly.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 33: FAMILY AND FRIENDLY IDENTITY THEFT FRAUD TREND

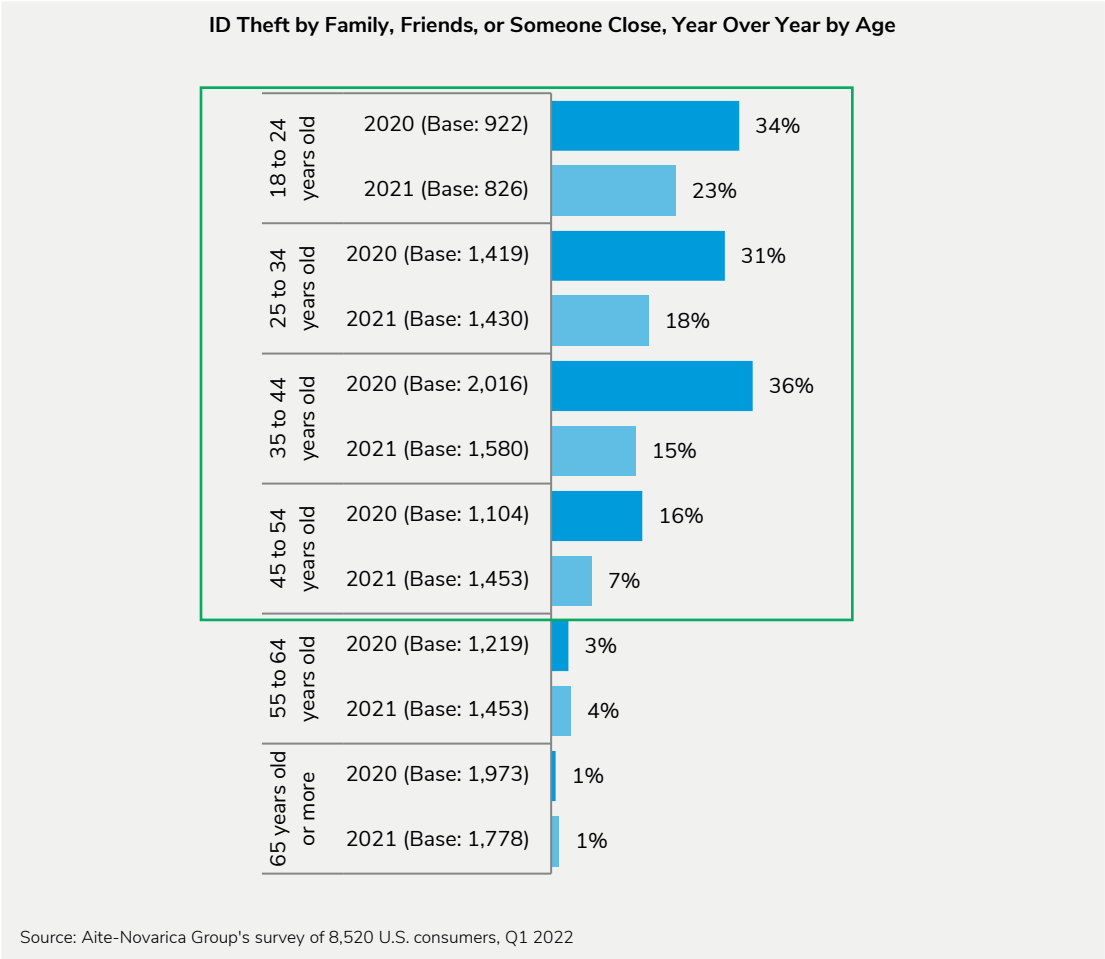


Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

The differences shown in Figure 34 in the first four categories (ages 18 to 54) are significant when comparing 2020 to 2021. In those age categories, total identity theft committed by family and friends decreased significantly during 2021. Perhaps the changes in living conditions and employment improvement during 2021 relieved some of the economic stress that led to high fraud rates in 2020, as many industries began to rebound from the pandemic and stores and restaurants reopened.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 34: FAMILY AND FRIENDLY IDENTITY THEFT COMPARISON BY AGE

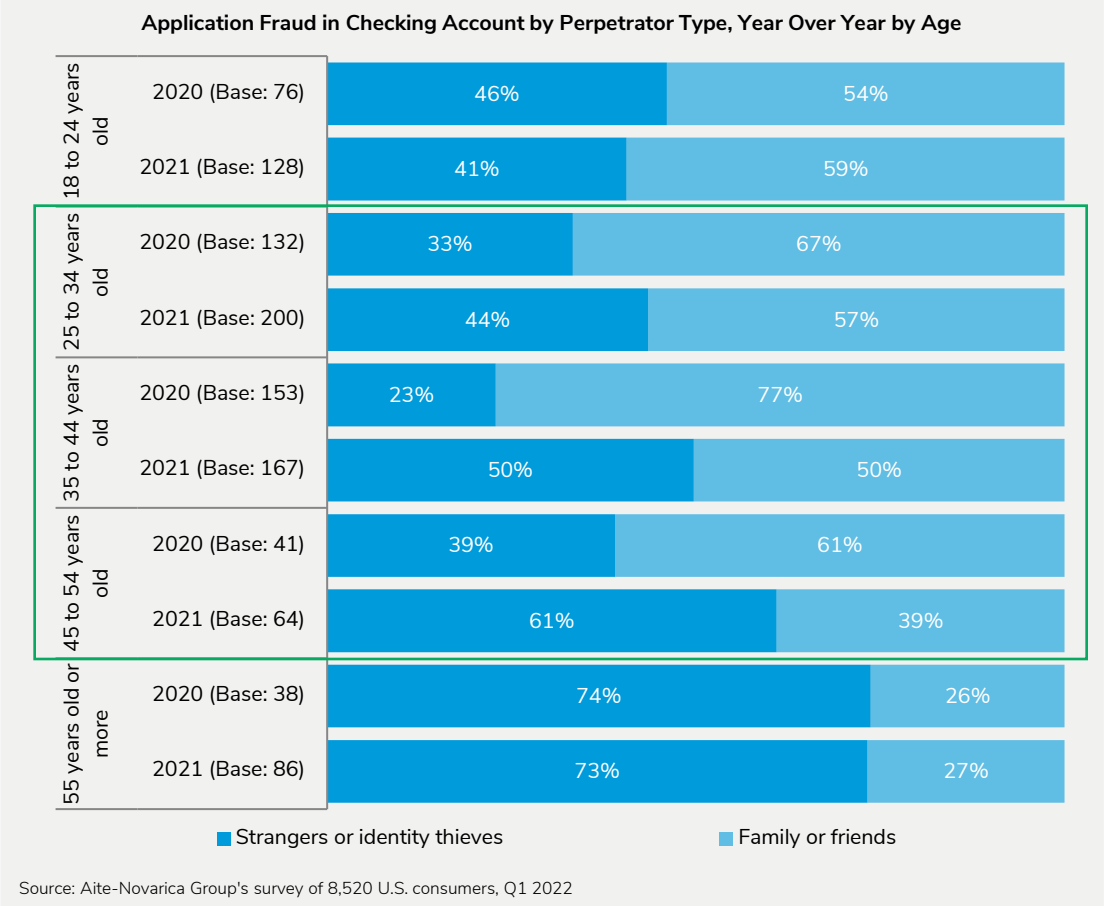


Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

Regarding checking account application fraud, identity theft victims between the ages of 25 and 54 experienced a significant increase in fraud committed by friends and family in 2021 compared to 2020 (Figure 35). This age group led to this category of increased application fraud in 2021, when many other types of application fraud decreased.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 35: YEAR-OVER-YEAR FRIENDS AND FAMILY FRAUD RATES



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

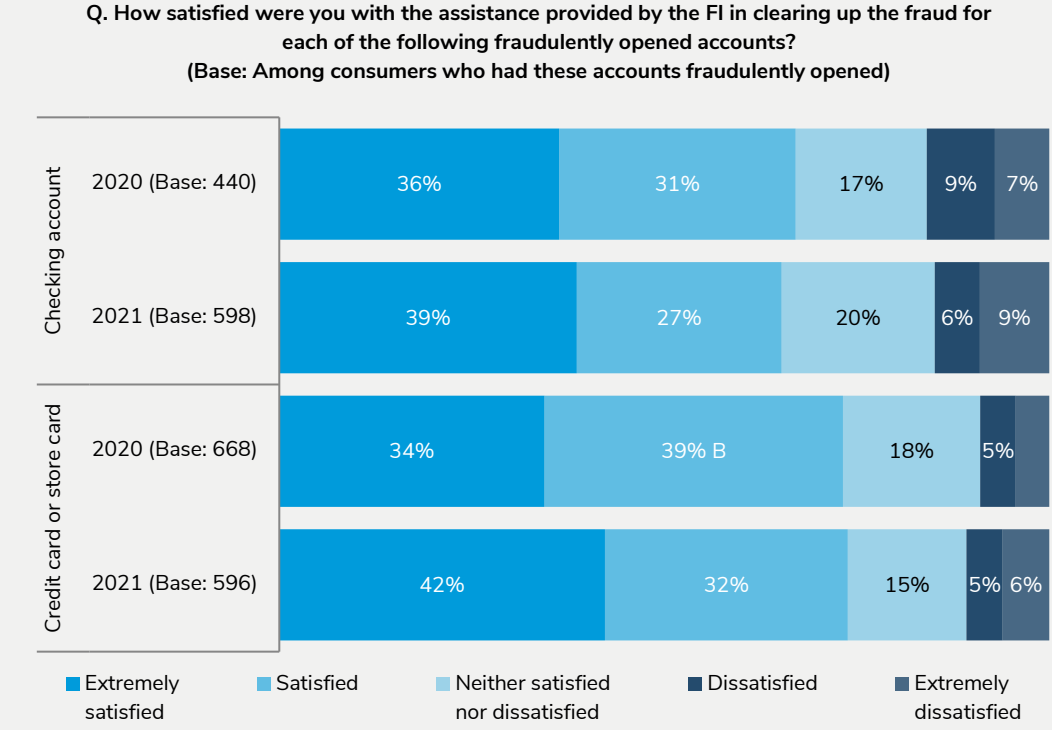
Credit card application fraud by family and friends showed a similar trend in these same age groups, with 2021 incidents increasing significantly over 2020.

SATISFACTION LEVELS

Consumer satisfaction levels were similar in 2021 and 2020 regarding FI assistance provided to application fraud victims for checking accounts and credit cards (Figure 36). However, in 2021, consumers were more likely to describe themselves as extremely satisfied when it came to application fraud in credit cards or store cards. Perhaps consumers have become a little more forgiving due to the pandemic. Dissatisfaction rates were also similar in both years.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 36: COMPARISON OF SATISFACTION LEVELS FOR FI ASSISTANCE

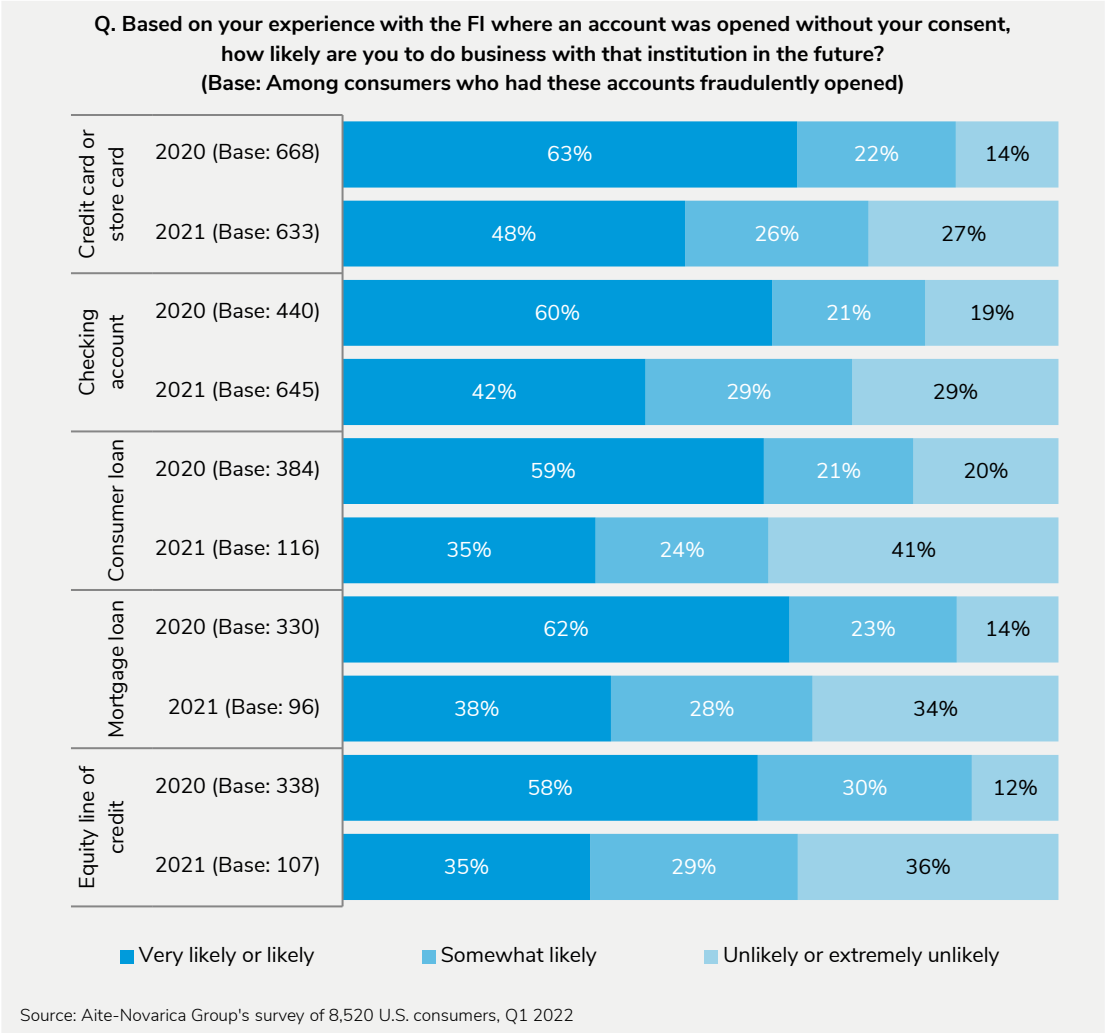


Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

Consumers are far less forgiving when it comes to doing business in the future with an FI where application fraud occurred. Consumers are less likely to do business at the FI that opened the fraudulent account in the future, regardless of the type of account opened (Figure 37). In 2020, 63% of application fraud victims for credit cards said they would likely do business with the FI that opened the card accounts in the future, compared to only 48% who said they were likely to do so in 2021.

© 2022 Aite-Novarica Group. All rights reserved.

FIGURE 37: LIKELIHOOD OF CONSUMERS DOING BUSINESS WITH AN FI WHERE APPLICATION FRAUD OCCURRED



Source: Aite-Novarica Group's survey of 8,520 U.S. consumers, Q1 2022

© 2022 Aite-Novarica Group. All rights reserved.

RECOMMENDATIONS

Firms have a responsibility to know whom they are doing business with and protect their customers against fraud to the extent possible. The methods fraudsters use to commit identity theft continue to evolve and grow more sophisticated. Firms that don't upgrade their fraud strategies over time will not be effective in combating fraud. Strong application controls can help protect innocent consumers, and strong controls to authenticate returning customers can protect against ATO incidents. Protecting against all forms of identity theft can protect a firm against potential financial loss, reputational damage, regulatory problems, and customer attrition.

Identity theft:

- Review and enhance current application controls and Know Your Customer processes to protect consumers against identity theft. Doing so will help reduce fraud losses and improve regulatory compliance as well.
- Review and enhance existing controls to validate the identity of returning customers to protect against ATO.
- Technology is constantly improving with new and elevated fraud prevention capabilities available on the market. Learn about these new capabilities and update fraud strategies to take advantage of the ones that are needed.
- Evaluate and sharpen the investigative and resolution processes for identity theft victims. Ensure staffing is adequate to handle cases on a timely basis and that investigators treat victims with respect, listen carefully to their problems, and communicate well and resolve cases as quickly as possible.
- Evaluate feedback from recent victims to obtain ideas to improve processes, protocols, and systems.
- Increase the education delivered to customers about identity theft; educational materials should be inviting and interesting so consumers will want to read them.
- Offer more capabilities to enable consumers to help protect their accounts, such as alerts on accounts, cards that can be turned off if not being used, etc. Provide consumers with opportunities to collaborate in protecting their accounts.

© 2022 Aite-Novarica Group. All rights reserved.

RELATED AITE-NOVARICA GROUP RESEARCH

Scams: On the Precipice of the Scampocolypse, March 2022

Market Trends in Fraud for 2022 and Beyond: New Fraudsters, New Era, February 2022

U.S. Identity Theft: Consumer Trends in Health, Life, and P&C Insurance, June 2021

U.S. Identity Theft: The Stark Reality, March 2021

Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise, February 2021

© 2022 Aite-Novarica Group. All rights reserved.

ABOUT GIACT (A REFINITIV COMPANY)

GIACT (a Refinitiv company) is a leader in helping companies positively identify and authenticate customers. GIACT empowers organizations across industries with data-driven insights, providing a multi-dimensional view of consumer and business identity, payments and compliance risk. GIACT's end-to-end, single API solution—the EPIC Platform—protects organizations from a diverse range of threats across the customer lifecycle, from account opening and servicing, to payment processing and compliance. For more information, visit www.giact.com or call 1-866-918-2409.

© 2022 Aite-Novarica Group. All rights reserved.

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

CONTACT

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

AUTHOR INFORMATION

Shirley Inscoe
+1.617.398.5050
sinscoe@aite-novarica.com

Research Design & Data:
Sarah Fitzsimmons
sfitzsimmons@aite-novarica.com

© 2022 Aite-Novarica Group. All rights reserved. Reproduction of this report by any means is strictly prohibited. Photocopying or electronic distribution of this document or any of its contents without the prior written consent of the publisher violates U.S. copyright law and is punishable by statutory damages of up to US$150,000 per infringement, plus attorneys' fees (17 USC 504 et seq.). Without advance permission, illegal copying includes regular photocopying, faxing, excerpting, forwarding electronically, and sharing of online access.

© 2022 Aite-Novarica Group. All rights reserved.