Aite PARTNER. ADVISOR. CATALYST.

U.S. Identity Theft: The Stark Reality

MARCH 2021

Shirley Inscoe

TABLE OF CONTENTS

LIST OF FIGURES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- This Impact Report is based on online surveys with 8,653 U.S. consumers in December 2020 to understand various issues related to identity theft and new banking behaviors adopted due to the COVID-19 pandemic.
- Forty-seven percent of U.S. consumers experienced financial identity theft (application fraud in their name or account takeover [ATO]) in the past two years.
- Losses due to identity theft increased by 42% from 2019 to 2020 primarily due to the COVID-19 pandemic. Aite Group estimates that losses from identity theft will grow to US$635.4 billion by 2023.
- Thirty percent of consumers report it took them over 100 hours to recover from their identity theft incident.
- The largest age group of consumers (30%) who were identity theft victims in the past year were between 35 and 44 years of age.
- Application fraud occurs when a fraudster uses another individual's personal information without their consent or knowledge to open a new account, file taxes, or apply for benefits (e.g., insurance or governmental). Thirty-seven percent of U.S. consumers were victims of application fraud in the past two years.
- At least 10% of consumers in every application fraud category listed were dissatisfied with the recovery process.
- There is no segment of application fraud in which the recovery effort is consistently easy, since some portion of consumers in every category took a year or longer to finish the process.
- Twelve percent to 13% of consumers are unlikely to do future business with a financial institution where a checking account, credit card, or loan was opened in their name, even if they are satisfied with the assistance provided by the FI. However, among those who were dissatisfied with the assistance provided to them, between 42% (credit card) and 56% (consumer loan) of consumers are unlikely to do business with the FI in the future, depending on the type of account involved.
- Thirty-eight percent of U.S. consumers experienced ATO in the past two years.
- At least half of ATO victims know the person who took over their account. As FIs educate consumers, they need to emphasize family and friendly fraud, since it is so widely prevalent.
- Attrition can occur after an ATO incident because consumers lose confidence that their FI can protect their account; some of the attrition can be avoided if the FI detects the fraud before customers detect it.
- At least 85% of consumers who used online or mobile banking for the first time were satisfied.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- At least 82% percent of consumers who used online or mobile banking for the first time plan to continue to use the new delivery channel in the future.
- Very similar percentages of consumers believe they are knowledgeable about fraud scams, whether they experienced identity theft (61%) in 2020 or not (57%).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

"Like other forms of stealing, identity theft leaves the victim poor and feeling terribly violated."[1] *—George W. Bush*

Many consumers fear becoming victims of identity theft. Everyone has heard horror stories of how difficult it is to recover from an imposter stealing your identity, amassing debt, or causing other problems. It can take months or years to recover from being victimized, and then the thief can strike again. After all, the thief still has all the consumer's personal information. While a phone number or even physical address can be changed if a consumer is motivated, no one can change their birthdate or Social Security number.

Market confusion has led to differences in opinion as to what actually constitutes identity theft. For the purpose of this report, identity theft comprises application fraud (when an unauthorized person uses a consumer's identity to open new accounts, file for governmental benefits, or perform other activities as though they were the true person) and ATO (accessing a person's existing account or other asset in an unauthorized manner in order to steal funds, rewards, or benefits). This report examines how victims are impacted in the real world. It sizes the problem of identity theft in the U.S. and differentiates it from a simple fraudulent credit card transaction. This report also examines how consumer banking behaviors changed as a result of the COVID-19 pandemic and whether consumers will continue new digital behaviors adopted during the pandemic in the future or revert to their old patterns of activity. In addition to fraud and retail bank executives who will find these topics to be of interest, executives responsible for digitization efforts, customer experience, and brand reputation will find this report beneficial.

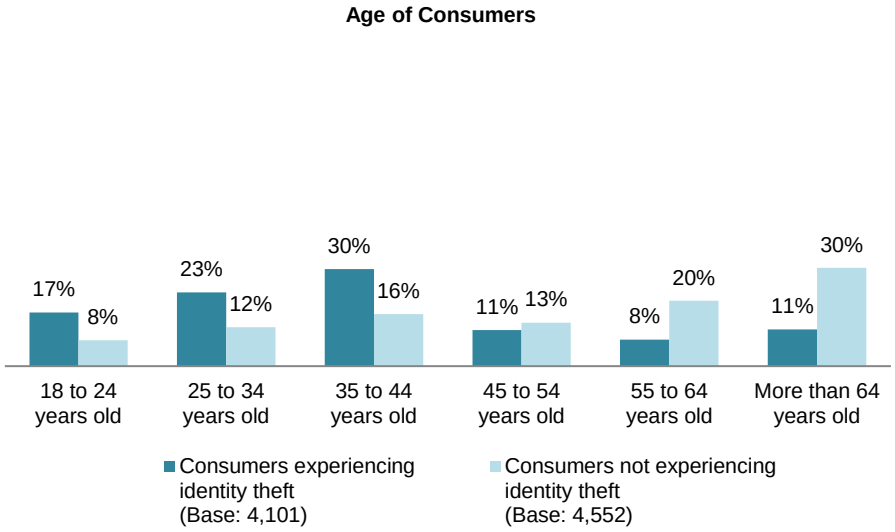
METHODOLOGY

GIACT, an industry leader in payments and identity fraud prevention, commissioned Aite Group to conduct an online quantitative survey in December of 2020, and 8,653 U.S. consumers aged 18 or older were surveyed. 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 have a margin of error of approximately 3 points at the 99% confidence level. Statistical tests of significance, 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. While no one is exempt from identity theft, the highest percentage of consumers (30%) who were victimized in the past year were between 35 and 44 years of age (Figure 1).

1. "President Bush Signs Identity Theft Penalty Enhancement Act," July 15, 2004, accessed January 21, 2021, https://georgewbush-whitehouse.archives.gov/news/releases/2004/07/text/20040715-3.html.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 1: Age of Respondents



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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THE MARKET

Identity theft is a hot topic in the market, and many consumers are fearful of being victimized. Consumers have heard about numerous data breaches in recent years, many of which caused some of their own information to be breached, and they have heard horror stories about how common identity theft is and how painful the recovery process can be. Almost everyone has been a victim of identity theft or knows someone who has. The term "identity theft" is often used inappropriately to include a single unauthorized credit card transaction; this inclusion undermines the severity of true identity theft. Identity theft occurs when a consumer's personally identifiable information (PII) is used to apply for a new account, file taxes, obtain a mobile phone, or other activity, or when a consumer's identity is used by an impersonator to take over an existing account. In general, cases of true identity theft are more difficult and time-consuming to recover from, and may require filing a police report, completing an affidavit, or performing other processes that are not required for just an unauthorized credit card transaction. Victims sometimes state they are made to feel like a criminal during the recovery process, even though they have done nothing wrong (Table A).

Table A: The Market

Market trends	Market implications
Inconsistent use of the term "identity theft" has led to market confusion as to what it really means.	One unauthorized credit card transaction does not constitute identity theft. Applications made for new products and services without the consumer's consent and impersonating a consumer to take over an existing account constitute identity theft.
Identity theft increasingly targets nonfinancial accounts.	Any type of account or benefit that is of value can be targeted by identity thieves (e.g., insurance, rewards programs, card on file at merchants, governmental benefits).
Consumers' PII has most likely been exposed due to all the data beaches in recent years.	Organized fraud rings gather data on consumers in databases and strike many individuals when they have aggregated enough information to apply for new products and services or successfully impersonate consumers to take over existing accounts.
The infrastructure in most firms is insufficient to reliably authenticate new applicants or existing customers consistently and correctly.	Identity crimes will continue to flourish until new methods of authentication are adopted across the industry. This also applies to phone carriers, insurance companies, firms that offer reward programs, and governmental agencies that oversee benefit programs and taxes.
Firms must invest in new technologies to prevent ongoing growth in identity crimes.	Utilizing technologies such as physical biometrics, behavioral biometrics, digital identities (that include devices), geofencing, and other new methods will enable more dependable and reliable authentication.

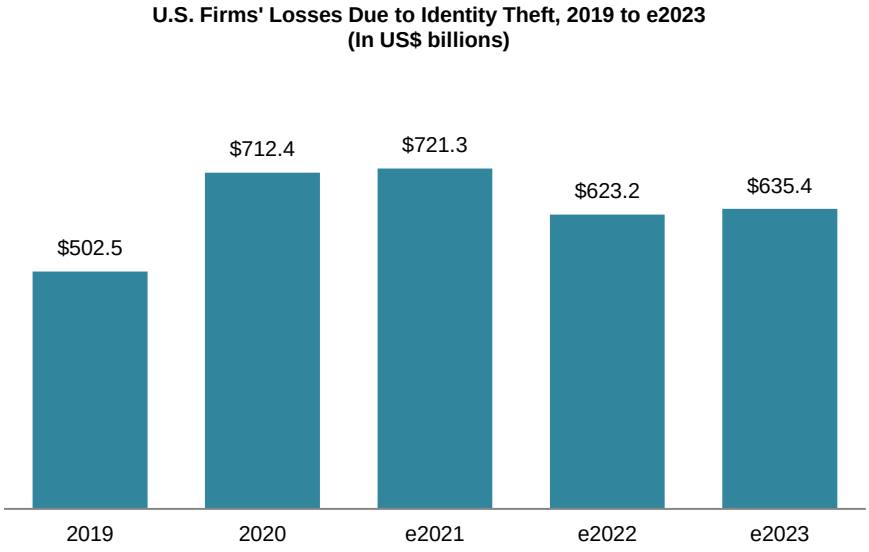
Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Identity theft is a growing problem in the U.S. In 2019, losses from identity theft cases were US$502.5 billion, and rapidly increased to US$712.4 billion in 2020, a 42% increase year-over-year. Identity theft losses grew very rapidly in 2020 (and will continue in 2021) due to the very high rate of unemployment identity theft during the pandemic. Unemployment benefits were increased, and the length of time to draw unemployment was extended, making this a very attractive target for fraudsters. After 2021, when life and unemployment benefits return to a new normal, identity theft losses will return to the same growth trajectory they would have been on had the pandemic not happened.

Aite Group projects that losses from all identity theft will grow to US$635.4 by 2023 (Figure 2).

Figure 2: Losses Due to Identity Theft Market Sizing



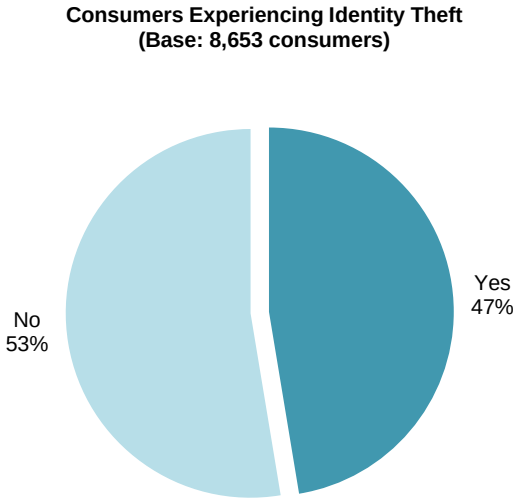
Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INCIDENCE RATE OF IDENTITY THEFT

Identity theft is a widespread problem, and consumers are largely unable to fully protect themselves from risk. With all the data breaches that have occurred in recent years across a variety of industries, consumers' PII is widely available to organized fraud rings. Phishing attacks, malware, and social engineering add to the wealth of data fraudsters have accumulated about consumers. Adding to the vulnerability, consumers are experiencing fraud committed by those familiar to them, friends and family who often have access to the same PII exposed in data breaches. Individuals cannot change their date of birth or Social Security Number, and changing addresses is often an unattractive option as well as expensive to undertake. Identity theft can take the form of what is often called "true identity theft," wherein someone uses another's identity to open accounts or apply for governmental benefits, or uses compromised credentials to impersonate the consumer in order to take over a financial account or rewards account, use insurance, or take advantage of other assets. In the past two years, 47% of American adults report being victims of some form of identity theft (Figure 3).

Figure 3: U.S. Identity Theft Victims in the Past Two Years

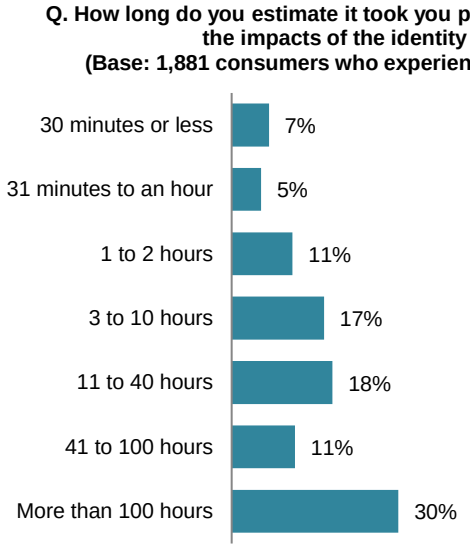


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

When identity theft occurs, victims typically go through emotional turmoil as they seek to recover from the incident and reclaim funds, rewards, or other benefits that were stolen. This process is examined for application fraud and ATO separately later in this report; the time required to recover from identity theft on average is shown in Figure 4. Thirty percent of consumers report it took them over 100 hours to recover from their identity theft incident. This shows the need for better processes and procedures to assist victims, particularly since these crimes are happening so often.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 4: Time Required to Recover From Identity Theft Incident



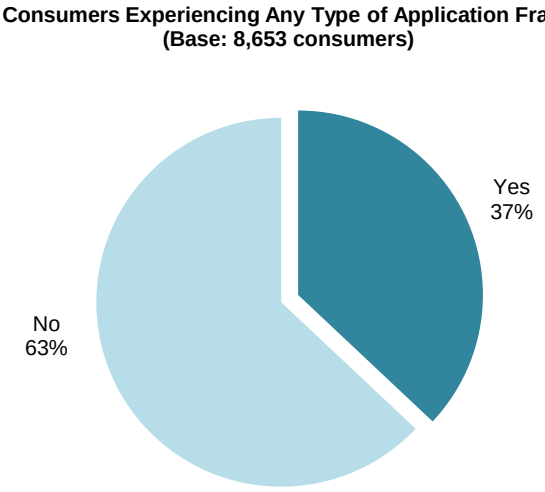
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

APPLICATION FRAUD

As explained earlier, assuming someone else's identity and using the victim's PII to apply for new accounts or services falls under application fraud—one form of identity theft. Fraudsters are very inventive and skilled at impersonating others to take advantage of what their victims have, be it money, rewards, insurance, or other assets. In the past two years, 37% of consumers have been victims of someone using their identity to open a new account of some type (Figure 5).

Figure 5: Application Fraud Victims



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

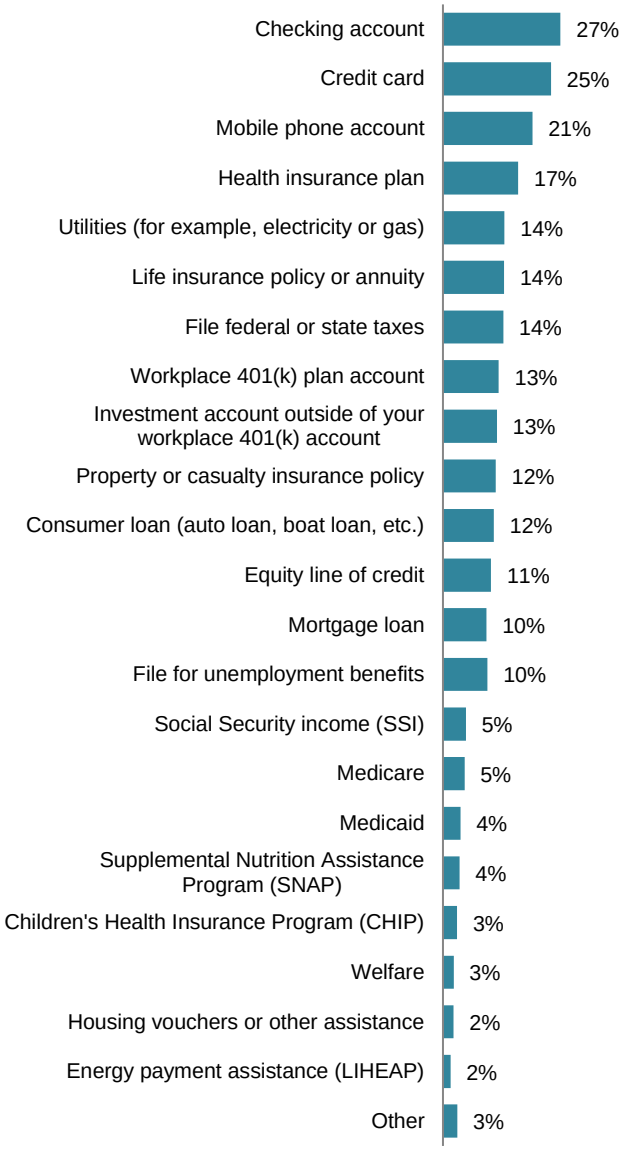
As detailed in Figure 6, the most common forms of application fraud include opening checking accounts (27%), credit cards (25%), or obtaining a mobile phone (21%). Big challenges for FIs related to application fraud include the creation and use of synthetic identities and first-party fraud related to identity theft.[2] Fraudsters often obtain a mobile phone prior to opening a new financial account so that they can use the phone number on the application; FIs are hesitant to open new accounts for people they cannot contact. But the list of types of application fraud is extensive—fraudsters obtained utilities in others' names (perhaps to avoid paying deposits), filed taxes to steal their refunds, obtained consumer loans, and even applied for mortgages and home equity lines of credit—in many cases, using houses the real owners were living in at the time. Fraudsters have no shame and will go to any length to benefit from the sound financial reputations others have established over the years.

2. See Aite Group's report *Synthetic Identity Fraud: Diabolic Charge-Offs on the Rise*, February 2021.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 6: Forms of Application Fraud Experienced by Victims

Q. During the past two years, has your personal information been used without your consent to open any of the following accounts or to apply for government benefits fraudulently? This is also known as identity theft. (Base: 8,653 consumers)



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

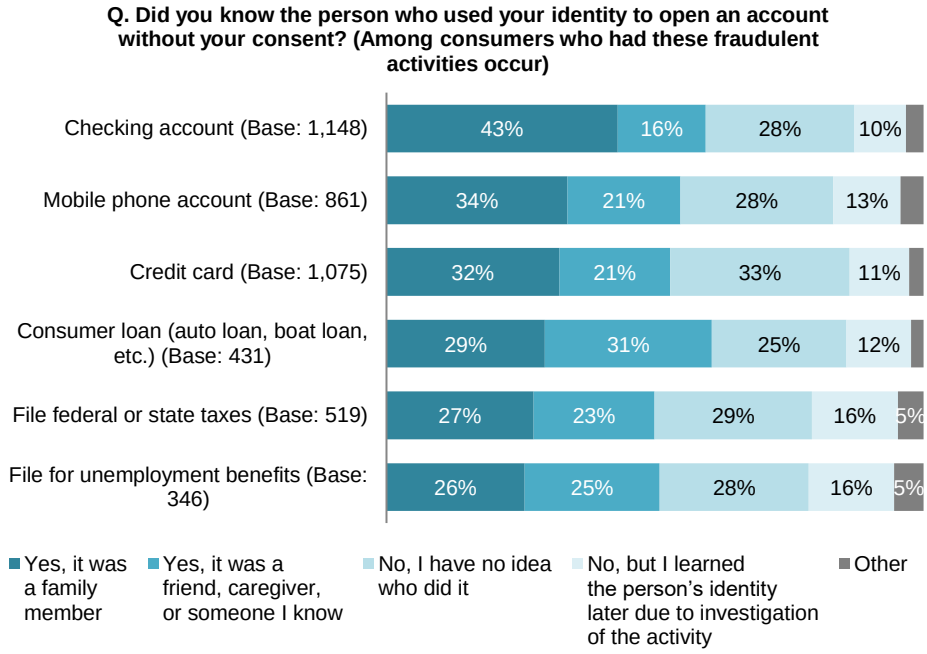
It is sad but true that in many cases, identity theft victims know the person who used their identities to apply for new products, services, or benefits. In every case, at least half of the victims of every type of application fraud were victimized by a family member, friend, caregiver, or someone else they know (Figure 7). While being victimized is always bad enough, knowing that someone you trusted and possibly loved did this to you has to add to the emotional toll of such an event.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

In today's society, many functions are performed online instead of face-to-face, and it has become very easy for people with access to the required information to impersonate others. People in the victim's home often have access to the victim's PII, account statements, and other confidential information. Consumers may even write down their online credentials where family members, roommates, and others can find them; similarly, many consumers use the same credentials for online activity across accounts, so if someone close to them learns what the credentials are for one website, that individual may try the credentials on other websites. The U.S. population continues to age, so elder abuse is likely to grow. While nobody wants to think that people they love will take advantage of them, this is an area in which more consumer education is badly needed.

The double whammy of having to contest the results of the abuse itself, coupled with the emotional distress of dealing with the fact that you can no longer trust those close to you, and realizing the fraud may happen again, can be debilitating. Similar to people who have been burglarized, identity theft victims describe feeling that they have been violated and often feel vulnerable or emotionally traumatized after being victimized.

Figure 7: Identity of Fraudsters Who Committed Application Fraud



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

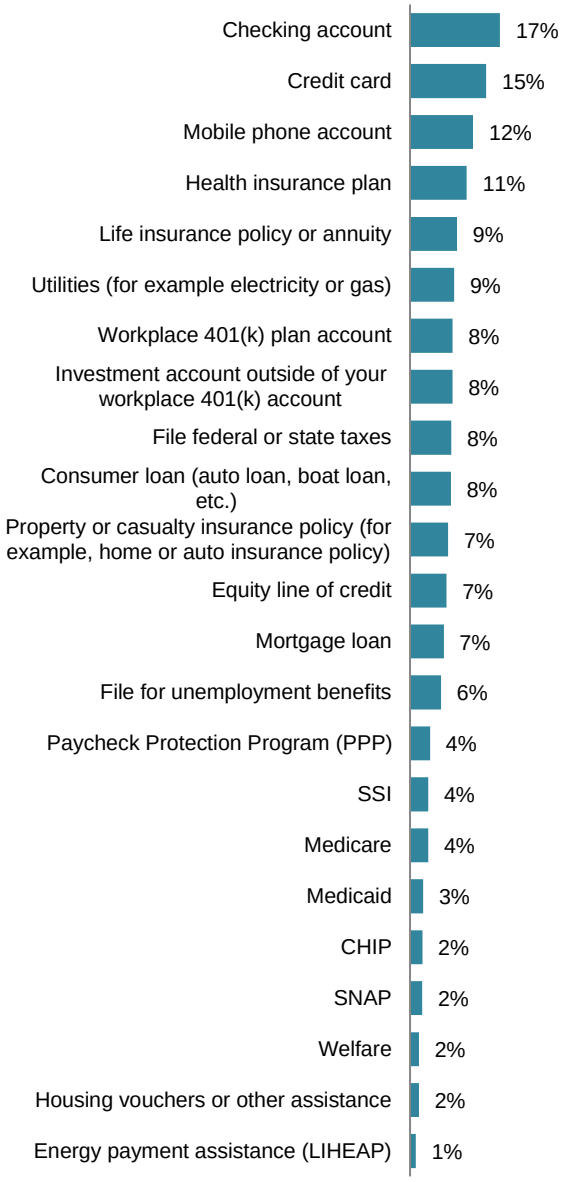
Family and friendly fraud is a very real problem; those people close to consumers often have access to their PII and can easily use it to open new accounts, file for benefits, etc. While the application rate for checking accounts (27%, as shown in Figure 6) seems high, that category showed the highest rate (17%) of application fraud by people known to the consumer (Figure 8). Credit card accounts are second at 15%, possibly fueled by offers received in the mail; these could easily be used by others with access to the family mail. Family and friendly fraud has been growing in recent years and will continue to increase unless consumers are better educated

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

about being careful to secure their information, even within their own homes. In most types of application fraud, half or more of the fraud is perpetrated by those known to the victim.

Figure 8: Family and Friendly Application Fraud Rates

Q. During the past two years, has your personal information been used without your consent to open any of the following accounts or to apply for government benefits fraudulently?
(Base: 8,653 consumers; Only consumers experiencing family and friendly fraud)



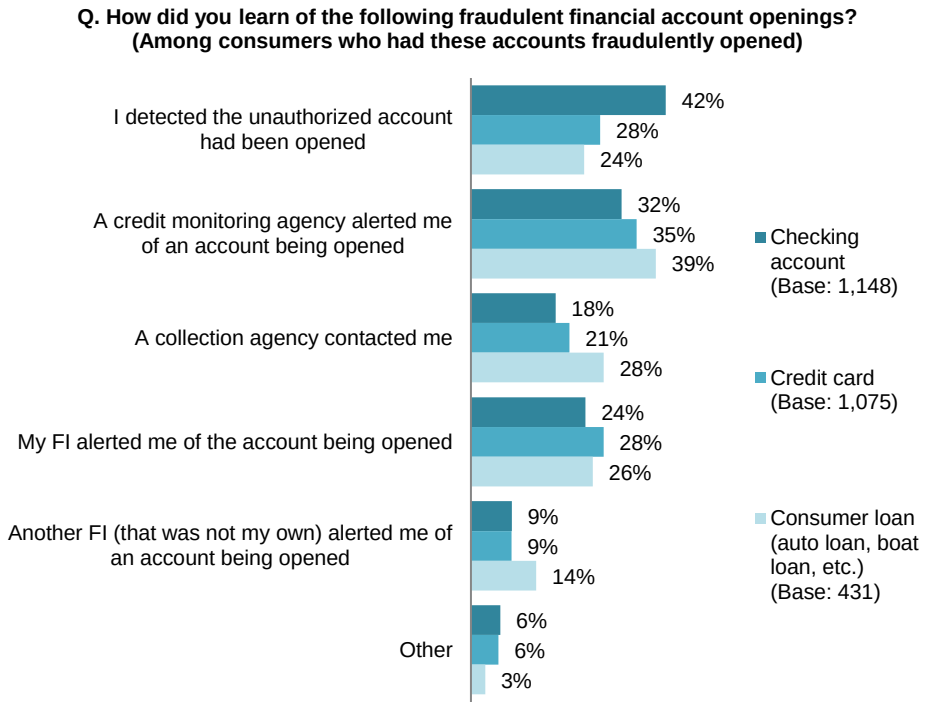
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Victims who had various financial accounts opened in their name without their consent learned of the fraud in different ways. In the case of a new checking account, 42% identified the fraud

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

themselves, 32% were notified by a credit monitoring service, 18% were contacted by a collection agency, and 33% were contacted by an FI (their own or the FI where the account was opened). For credit cards and consumer loans, the largest groups were notified by a credit monitoring agency—35% and 39%, respectively. Twenty-one percent of those who had a credit card opened in their name learned of the crime when they were contacted by a collection agency; similarly, 28% of those who had a consumer loan taken out in their name learned of the theft when contacted by a collection agency (Figure 9). Victims of this type of identity theft sometimes claim they are treated like crooks (when they dispute the debt) by skeptical collection agencies or FIs that think they are just trying to avoid repaying a debt.

Figure 9: How Victims Learned of Application Fraud



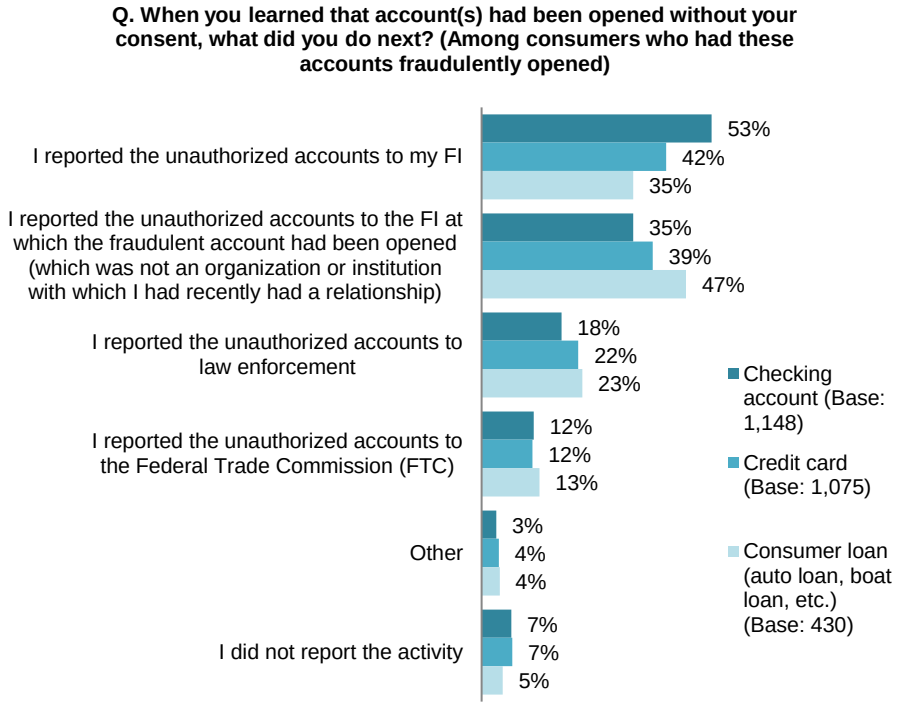
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Many consumers are not knowledgeable about the best steps to take subsequent to learning they have been victims of identity theft. They may look to an FI for direction since they aren't sure what to do. Victims are often emotional and vulnerable, particularly if they realize someone close to them has committed the crime. Often, investigators may initially doubt that the consumer was truly victimized and may push to prosecute the person who committed the crime; the victim, while being shocked by the identity theft, may still not want a loved one prosecuted, so it can result in a very complex situation.

The largest percentage of victims reported the identity theft to their own FI or to the FI where the new account was opened, regardless of what type of account was opened (Figure 10). Between 18% and 23% of victims reported the crime to law enforcement; some FIs may require a report to law enforcement as part of the fraud investigation process.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 10: Steps Taken Subsequent to Discovery of Identity Theft—Application Fraud



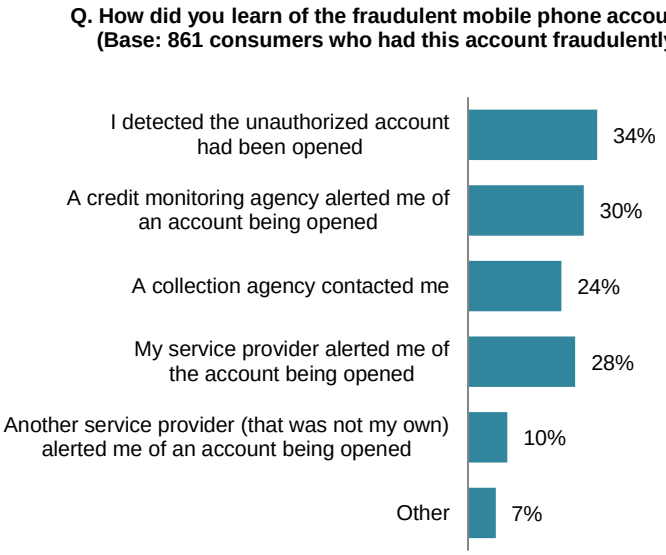
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Oftentimes, the first step in a fraudster's plan to commit identity theft or create a synthetic identity[3] involves obtaining a mobile device using the victim's PII. A mobile device is essential so that the company or governmental agency at which the fraudster is applying for an account or service can reach the fraudster easily. Over a third of consumers (34%) who experienced this type of identity theft detected it themselves. Thirty percent were notified by a credit monitoring agency, and 24% were contacted by a collection agency. Thirty-eight percent were notified by either their own mobile carrier or another one (Figure 11).

3. See Aite Group's report *Key Trends Driving Fraud Transformation in 2021 and Beyond*, December 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 11: Mobile Phone Identity Theft

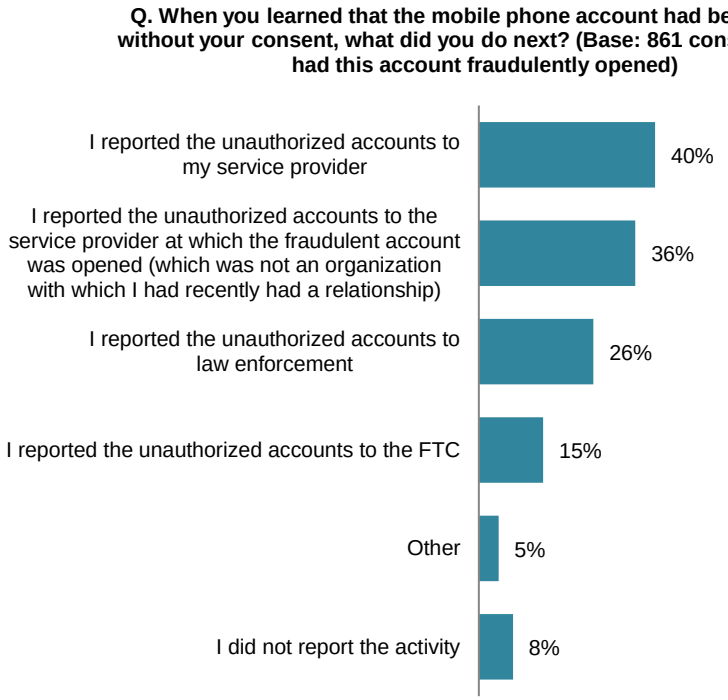


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Forty percent of consumers who were victims of identity theft related to new mobile accounts reported the incidents to their mobile carrier. In addition, 36% reported the unauthorized account to the mobile carrier where it was opened. Twenty-six percent reported the activity to law enforcement; only 15% reported the identity theft to the FTC (Figure 12).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 12: Steps Taken Subsequent to Discovery of Identity Theft—Mobile Phone

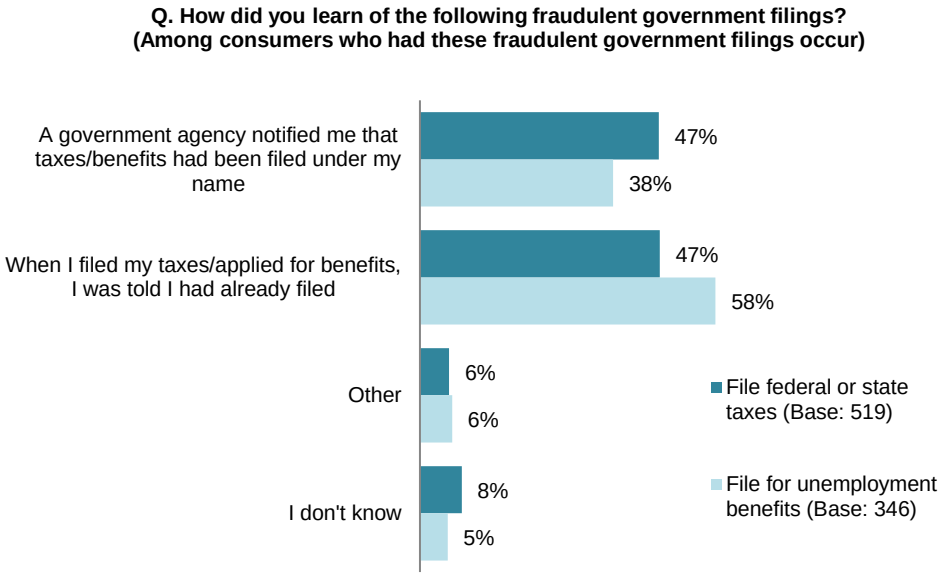


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

A variety of types of governmental benefits can be stolen via identity theft fraud when others impersonate the true consumer and file in their name. Figure 13 shows two such items: filing tax returns and unemployment benefits. The two primary methods of learning of this type of fraud are notification from a governmental agency or being told there is a previous application when a consumer attempts to file.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

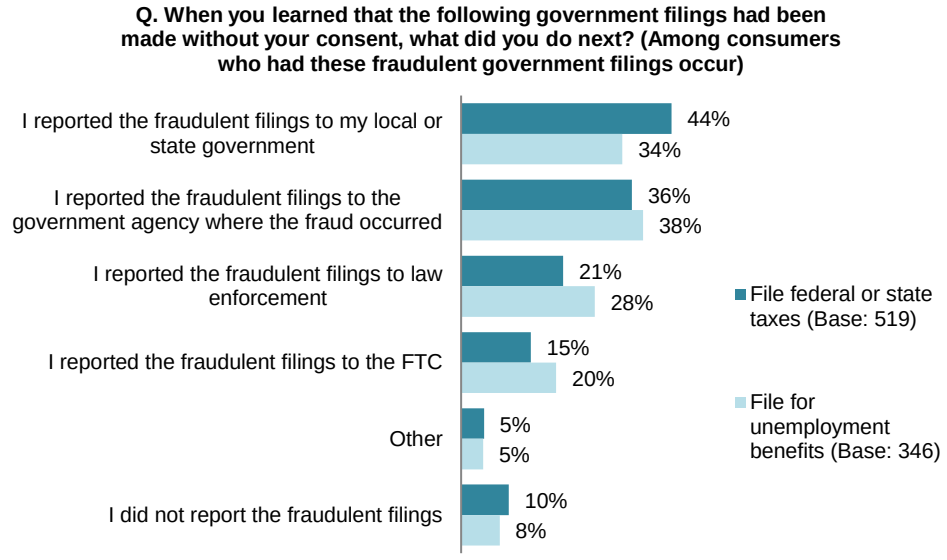
Figure 13: Identity Theft Related to Governmental Agencies or Benefits



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

Many consumers react to cases of identity fraud involving taxes or other benefits by reporting it to the governmental agency involved in the fraud, whether this is a tax agency or an unemployment department. Between 21% and 28% also reported the crime to law enforcement, and 15% to 20% reported it to the FTC (Figure 14). State unemployment offices may be doing a good job of encouraging consumers to report to the FTC; 20% is the highest rate of any type of application fraud that was reported to that agency.

Figure 14: Steps Taken Subsequent to Discovery of Identity Theft—Governmental Agencies or Benefits



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

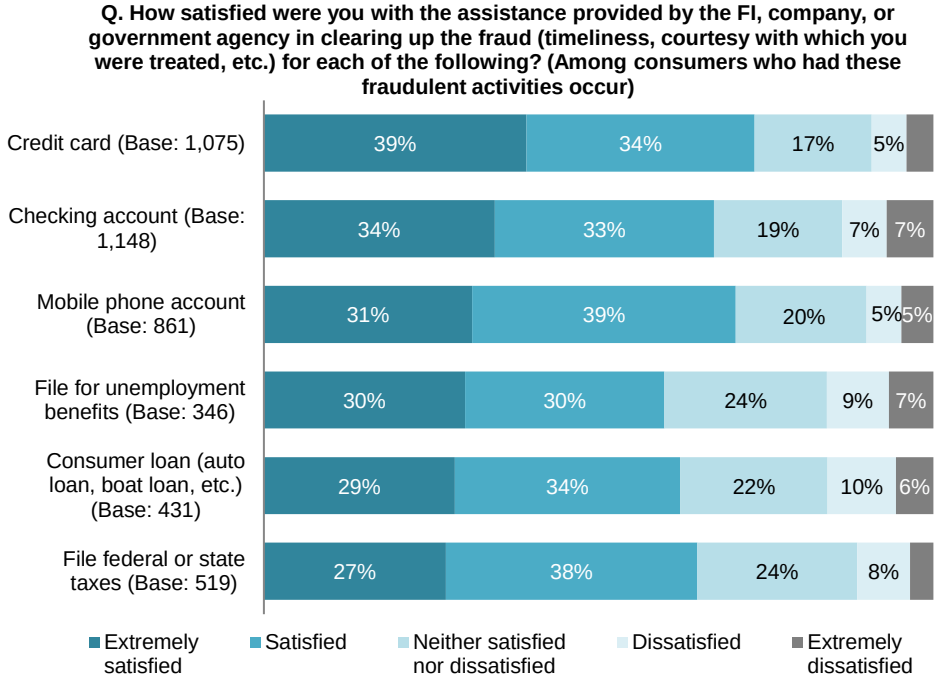
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

SATISFACTION WITH FRAUD RECOVERY PROCESS

Recovering from application fraud can be quite difficult because the entity where the new account was opened may not understand that it opened the account for a fraudster, not the true individual. As identity theft has become more common, many companies and agencies are becoming more familiar with this type of fraud and have developed better processes to assist victims quickly and easily. As these cases are investigated, it is vitally important that the investigator not rely on contact information provided by the applicant/fraudster, whether this be a telephone number, address, or email address; correct contact data must be used to communicate with the true consumer who has been victimized.

Sixty percent or more of respondents experiencing all types of application-related identity theft were at least satisfied with the process to dispute the unauthorized relationship. The highest satisfaction rates were reported by those who had credit cards or mobile phones obtained in their name. Conversely, consumers who were most dissatisfied with the recovery process were those for which thieves filed for unemployment benefits in their name or applied for loans or checking accounts. At least 10% of consumers in every application fraud category listed were dissatisfied with the recovery process (Figure 15).

Figure 15: Satisfaction Level With Recovery Process for Application Fraud



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

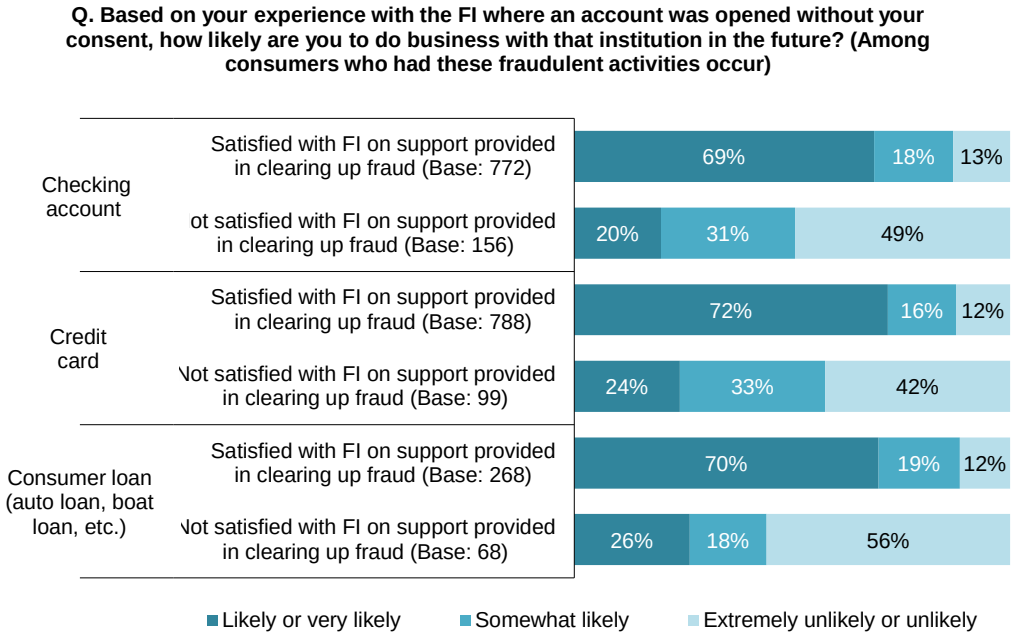
The way victims are treated as they dispute unauthorized new accounts can make a lasting impression with regard to the FI that opened that account. It shouldn't be surprising that consumers who feel they are not treated well by an FI during this process will be reluctant to do business with that particular FI in the future. Typically, consumers are also much more likely to relate negative treatment or experiences to friends and family than positive ones. If you consider

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

these factors, FIs that don't have good processes and procedures to assist identity theft victims recovering from this fraud may lose future business opportunities, not just from the victims themselves but also from others with whom they share their experience.

Twelve to 13% of consumers are unlikely to do future business with an FI where a checking account, credit card, or loan was opened in their name even if they are satisfied with the assistance provided by the FI. However, among those consumers who were dissatisfied with the assistance provided to them, between 42% (credit card) and 56% (consumer loan) are unlikely to do business with the FI in the future, depending on the type of account involved (Figure 16). While a small percentage of consumers are extremely dissatisfied with the treatment received, the memory of the treatment may cause them to refuse to do business with that provider for the rest of their lives. This opportunity cost of future business should be considered in training investigators handling these cases as well as during the development of procedures to be used.

Figure 16: Likelihood of Future Relationship



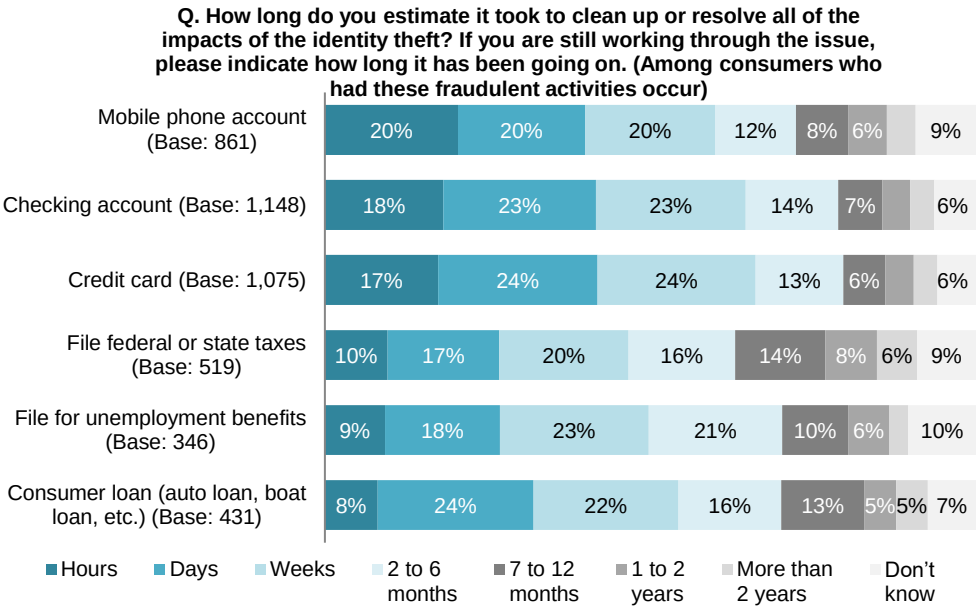
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

The amount of time required to recover from application fraud varies widely; part of this variance may be due to how often various firms or agencies deal with this type of fraud. Those that deal with it more often have likely developed procedures that enable consumers to recover more quickly and easily. Clearly, there is no segment in which this recovery effort is consistently easy since some portion of consumers in every category took a year or longer to finish the process (Figure 17). Recovering from application fraud involving a credit card or checking account had the fewest consumers who took longer than a year to finish the process, but that is too long for any consumer to have to deal with such a situation. All FIs, companies, and agencies should develop processes to assist individuals contending with this type of identity theft, so cases are consistently resolved in less time. This will make life easier for the victims and improve

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

operational efficiency for all those firms that open unauthorized new accounts from time to time (despite efforts to avoid doing so).

Figure 17: Period of Time Required to Recover From Identity Theft



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

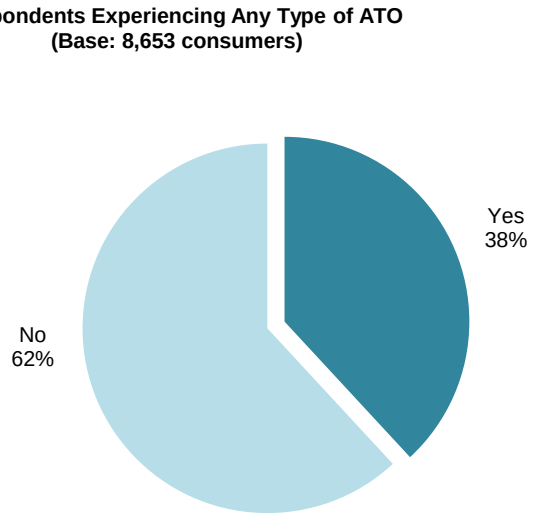
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ACCOUNT TAKEOVER FRAUD

In addition to application fraud, the other component of identity theft is ATO fraud. ATO occurs when a fraudster impersonates a customer and obtains unauthorized access to an existing account of any type (financial, government benefits, rewards, etc.). Once access is obtained, the fraudster can withdraw funds or utilize other assets owned by the legitimate consumer. ATO may be enabled by a call to the contact center where the fraudster successfully navigates authentication processes,[4] via online credentials that are obtained from a data breach, because a family member has access to the credentials, after fraudsters obtain account data through the interactive voice response system (IVR),[5] or by other methods.

Thirty-eight percent of U.S. consumers experienced ATO in the past two years (Figure 18).

Figure 18: ATO Victims in the Past Two Years



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

ATO can impact consumers in many different ways. In addition to accessing a financial account in order to steal money, fraudsters can access many other types of accounts owned by consumers, for example, rewards accounts for airlines, hotels, or merchants; insurance policies; or other accounts.

After successfully accessing an account, fraudsters take a wide variety of actions. If it is a financial account, the fraudster will likely use one of the payment systems (e.g., wire, ACH, or Zelle) to move funds out of the account to an account the fraudster controls. Fraudsters will sometimes (15%) change the contact information on the account so that if the transaction

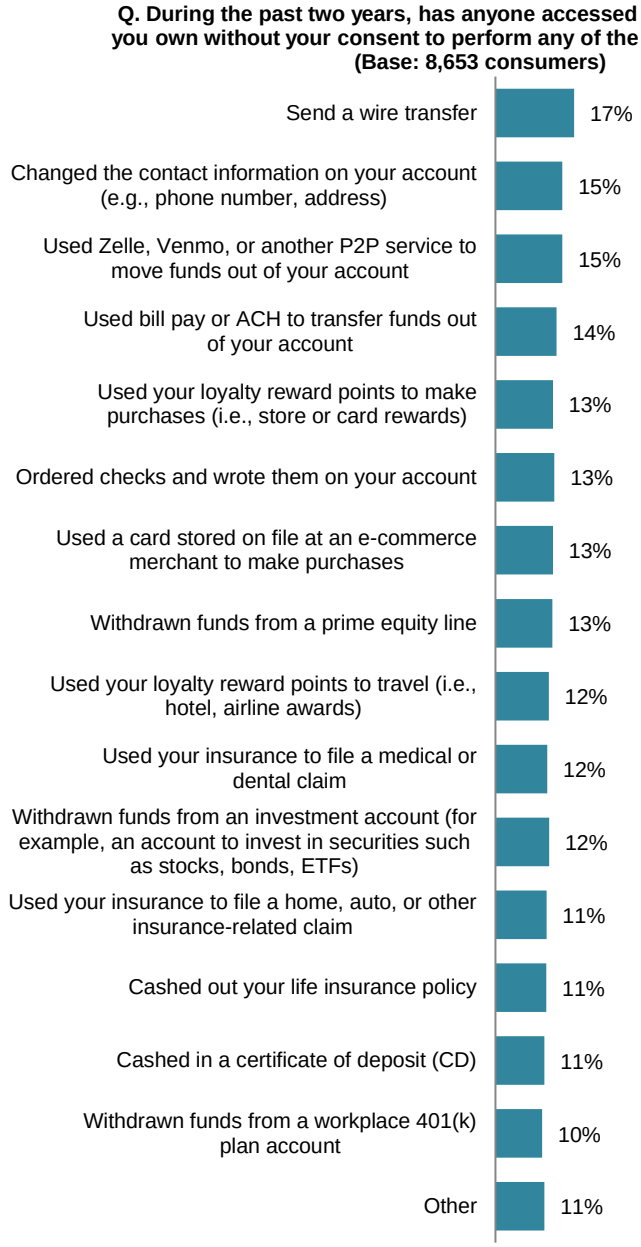
4. See Aite Group's report *Contact Centers: The Fraud Enablement Channel*, April 2016.

5. See Aite Group's report *Beating the Bad Guys: Safe and Secure Voice Interactions in the IVR*, November 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

appears suspicious to the FI, the FI will use the fraudster's contact info and be assured the activity is legitimate. All types of accounts are at risk for ATO; any account from which a fraudster can benefit is at risk. Fraudsters may use a person's medical insurance to cover their own medical expenses, travel with airline and hotel rewards accumulated by a consumer, run up an equity line on a home without the homeowner's knowledge, or commit other types of fraud (Figure 19).

Figure 19: Activities Performed After an ATO

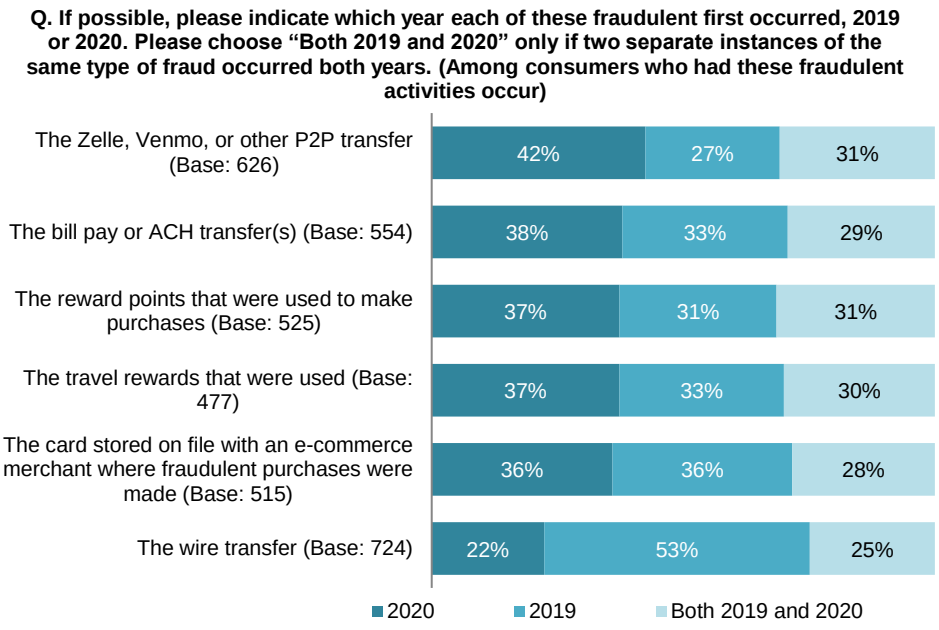


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Compared to ATO attacks in 2019, 2020 showed slight growth in most categories, with the exception that person-to-person (P2P) transfers were used far more often, and the use of wire transfers declined significantly. This is reflective of consumers' increasing use of real-time payments, such as Zelle and Venmo. While wire transfers also represent final payment, making stolen funds difficult to retrieve in the event of fraud, real-time payments move funds faster, often making them available for withdrawal by the thief before the originating FI or the account holder detects the fraudulent activity (Figure 20). The other significant observation is that many consumers were ATO victims in both 2019 and 2020.

Figure 20: Years in Which ATO Occurred

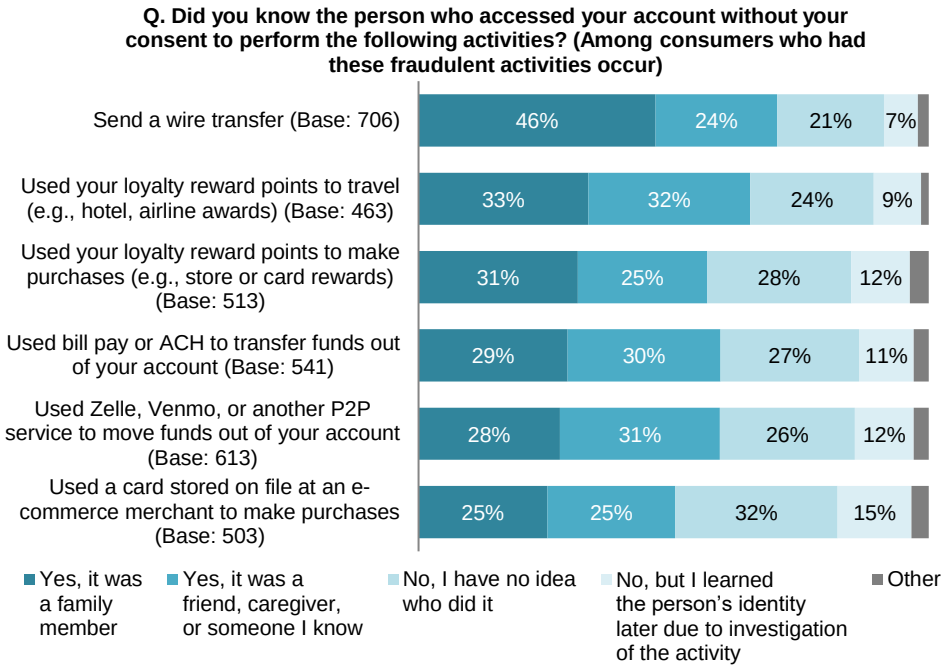


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Similar to application fraud victims, many ATO victims know the person who stole from their existing accounts. In fact, at least half of victims who had activities performed listed in Figure 21 knew the person who stole from their accounts. As FIs educate consumers, they need to emphasize family and friendly fraud more since it is so prevalent.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 21: Identity of Fraudsters Who Committed ATO



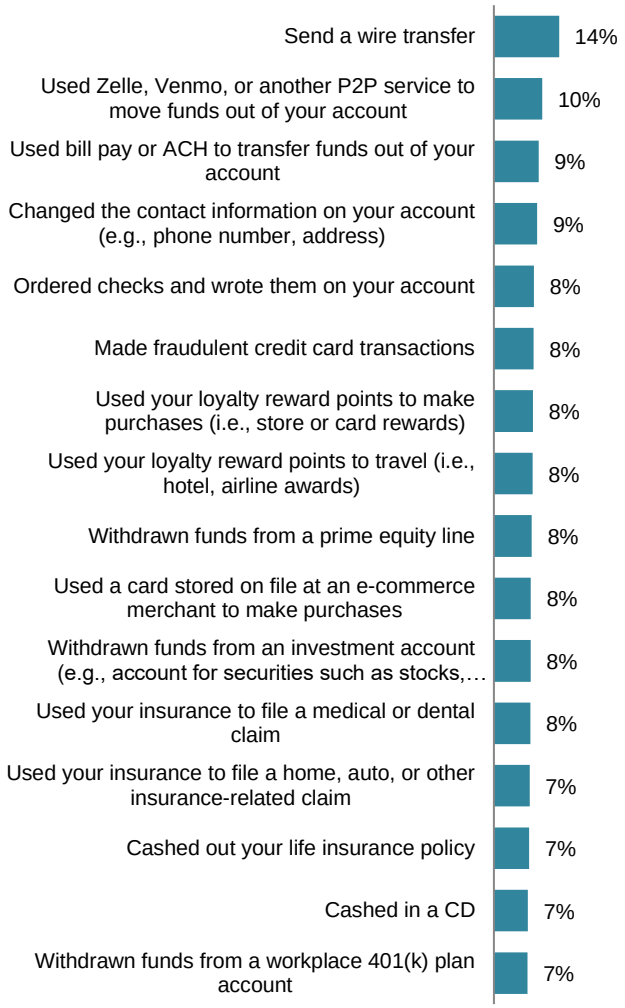
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Family and friendly fraud occurs more often with certain types of ATO fraud (Figure 22). Those committing this type of identity theft most often use wire transfers or P2P payments to move funds quickly and avoid having the transactions reversed. As shown in Figure 22, family members and friends commit all types of ATO. While all types of identity theft can leave victims feeling violated, having those you trust most steal from you has to add extra emotional baggage. It also may be more difficult for FIs to protect against this activity, particularly if it originates from the consumer's home address or even the consumer's personal device. ATO cases involving family members and friends may also take longer to investigate; some firms may be reluctant to reimburse the consumer unless they are willing to prosecute the one who committed the crime.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 22: Family and Friendly Fraud Rates for ATO

Q. During the past two years, has anyone accessed an existing account you own without your consent to perform any of the following activities? (Base: 8653 consumers; only consumers experiencing family or friendly fraud)

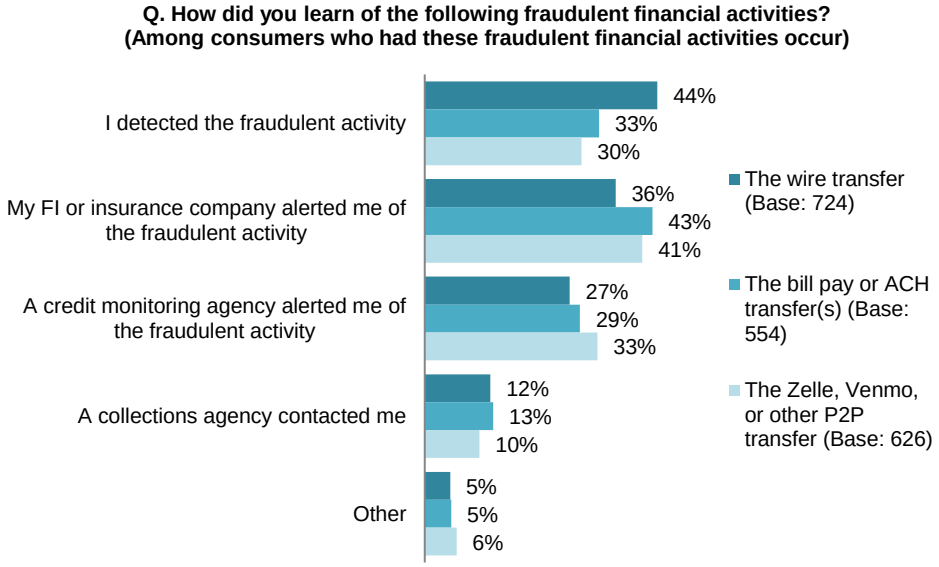


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Many consumers discover they have been victimized themselves by seeing unauthorized activity that has taken place on their accounts. Seeing a lower-than-expected balance in an account can alert a consumer to look more closely at all the transactions that have occurred. Other consumers learn of fraud by being alerted by the company where the account was taken over, a credit monitoring agency, or a collection agency (Figure 23).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

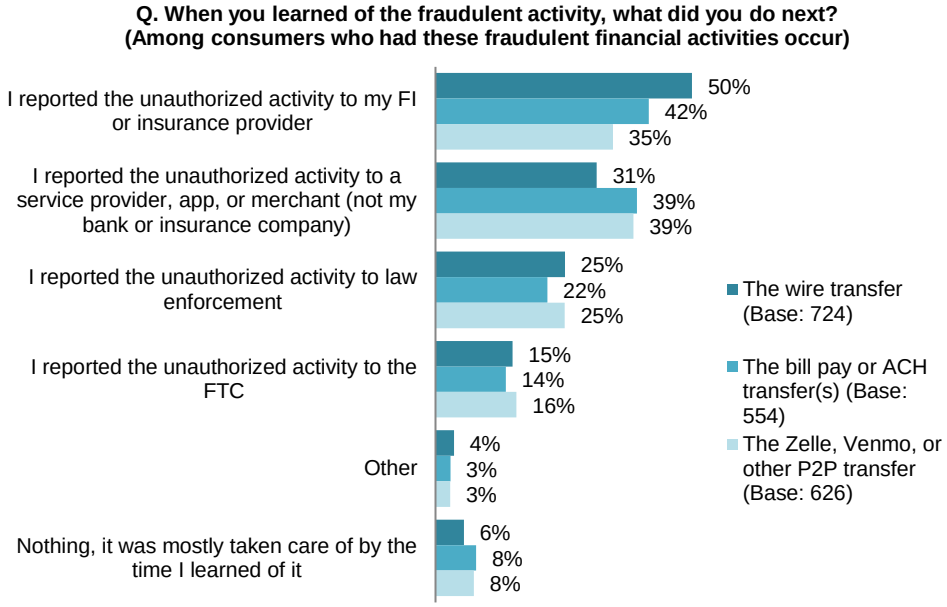
Figure 23: How Victims Learned of Financial ATO Incidents



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

Roughly a third to half of victims report ATO fraud to their FI or insurance company, or to another provider involved in the incident. Twenty-two percent to 25% report the incident to law enforcement; this may be a requirement by their FI or insurance company, or they may do so hoping the thief will be caught and prosecuted. Sixteen percent or less report the activity to the FTC; this may be an indication of lack of consumer education related to the FTC's role and could result in the FTC's data being badly understated when quantifying these crime rates (Figure 24).

Figure 24: Actions Taken After Learning of Financial ATO Incidents

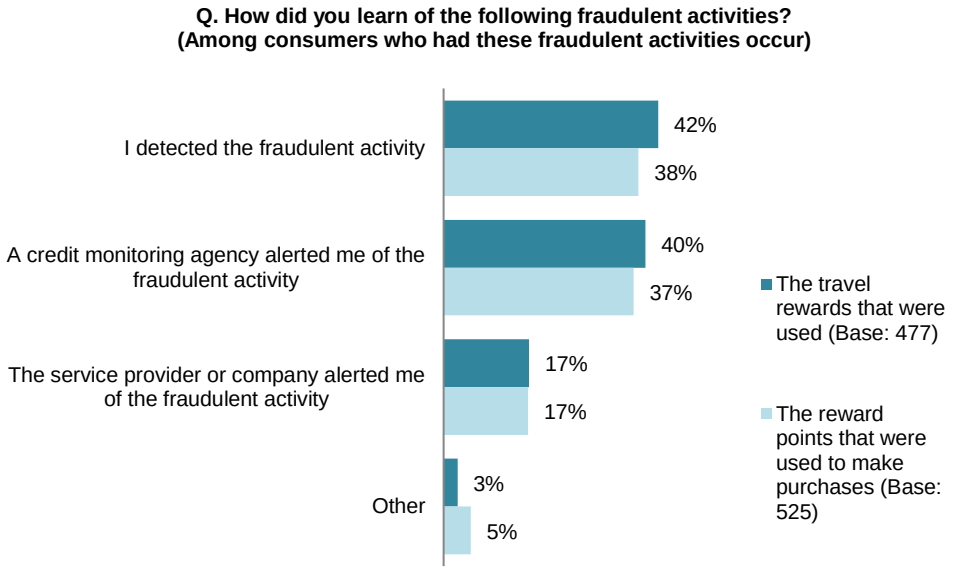


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

In cases in which consumers had reward accounts taken over, a similar percentage of people detected the fraud themselves as were alerted by a credit monitoring agency. Others were contacted by the service provider or company wherein the fraud occurred (Figure 25).

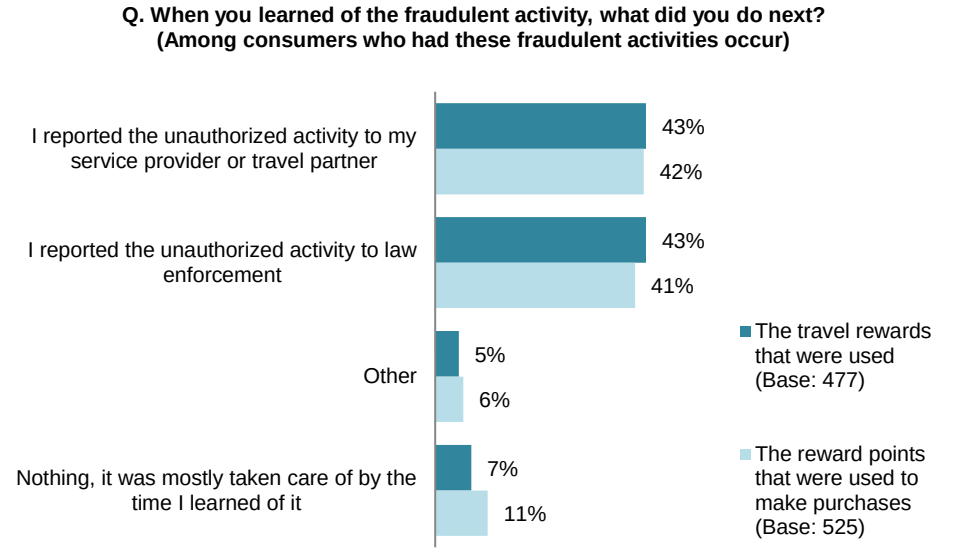
Figure 25: How Victims Learned of Rewards ATO Incidents



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

After learning that a rewards account had been taken over, 41% to 43% of consumers reported the ATO fraud to their service provider and/or to law enforcement (Figure 26).

Figure 26: Actions Taken After Learning of Rewards ATO Incidents

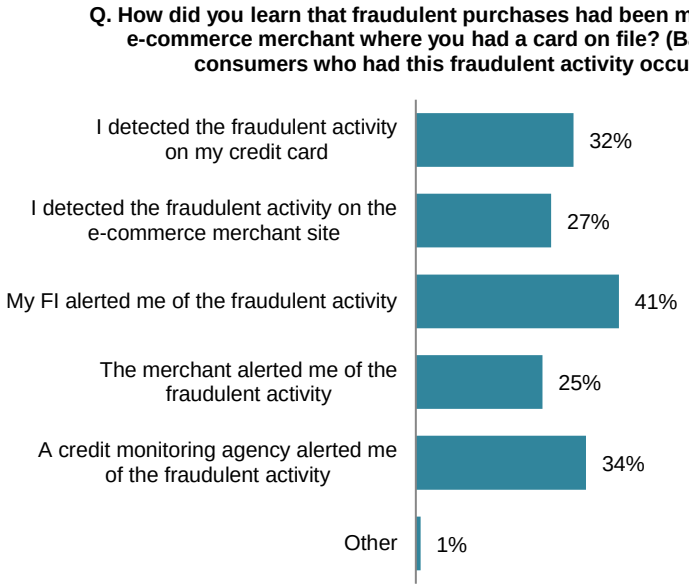


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Thirty-two percent of ATO victims who had a card stored with a merchant taken over discovered the theft by reviewing their credit card statement. Forty-one percent were alerted by their FI, and 34% were notified by a credit monitoring agency. Only a quarter of these victims were notified by the merchant where the card was on file (Figure 27).

Figure 27: How Victims Learned of E-Commerce Merchant ATO Incidents

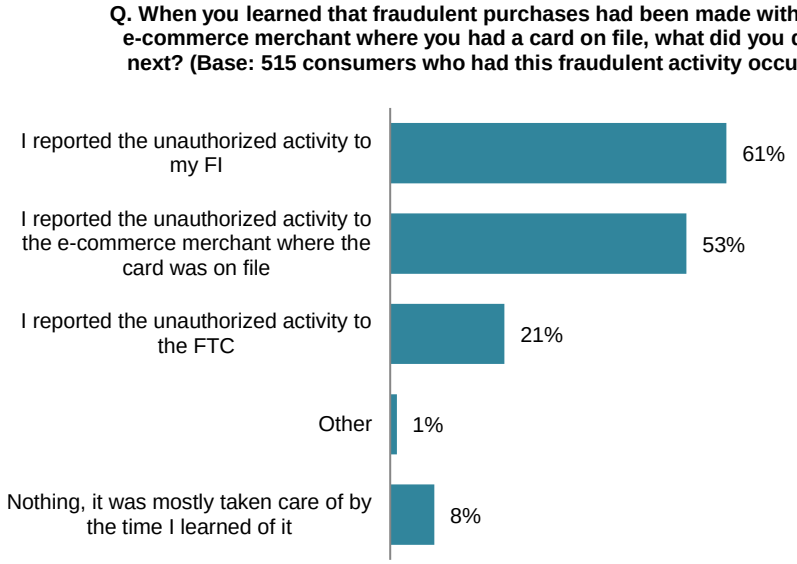


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

After learning of the e-commerce merchant ATO, 61% reported the theft to their FI, and 53% reported the fraud to the merchant where the card was on file. Twenty-one percent reported it to the FTC (Figure 28).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 28: Actions Taken After Learning of E-Commerce Merchant ATO Incidents



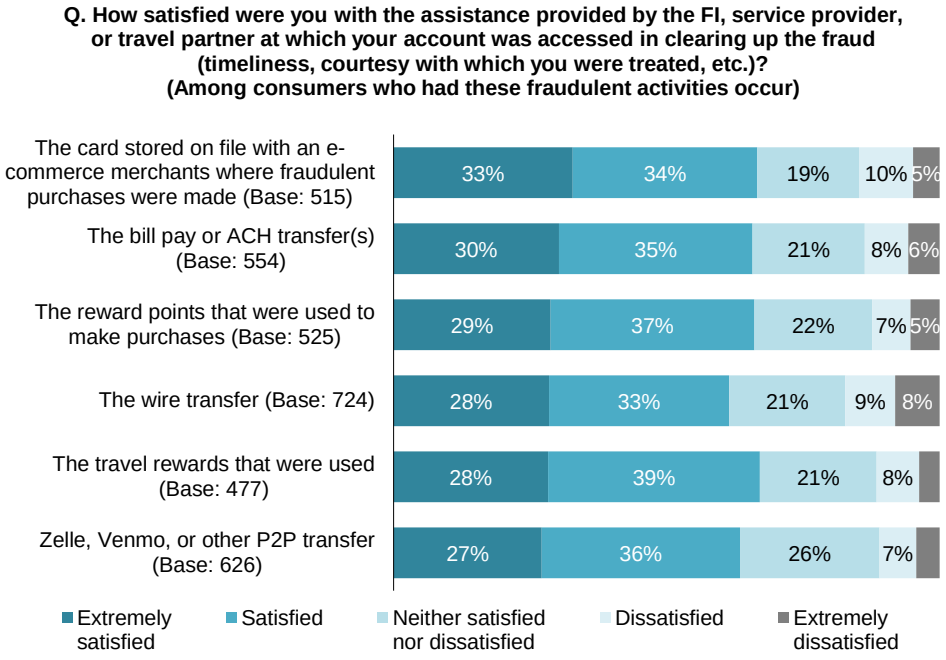
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

SATISFACTION LEVELS WITH ATO RECOVERY PROCESS

At least 61% of ATO victims were satisfied with the recovery process regardless of the type of account taken over. However, at least 10% were dissatisfied with the recovery process, and these consumers likely shared their bad experience with friends and family members. The category of ATO with the highest percentage of satisfied consumers is travel rewards, but all the categories are fairly similar (Figure 29).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 29: Satisfaction Levels With ATO Recovery Process

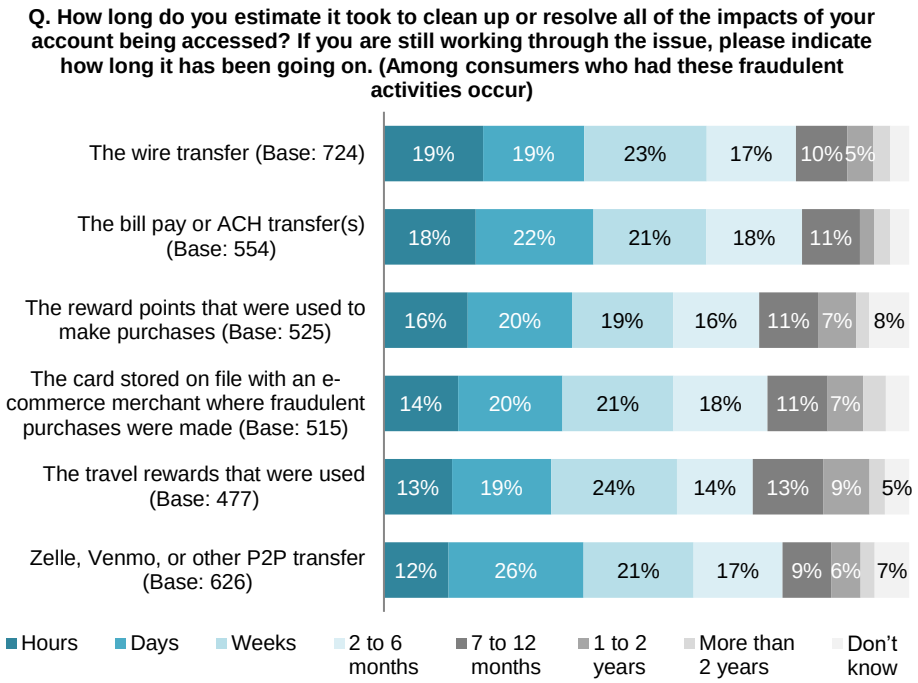


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

At least 32% of consumers in every ATO category were able to resolve their case of identity theft in a matter of hours or days. Overall, cases involving the theft of travel rewards, other rewards, and cards used that were stored at an e-commerce merchant took the longest to resolve. However, every category of ATO shows at least some consumers who spent more than two years trying to resolve the ATO fraud committed (Figure 30).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 30: Length of Time Required to Resolve ATO Incidents

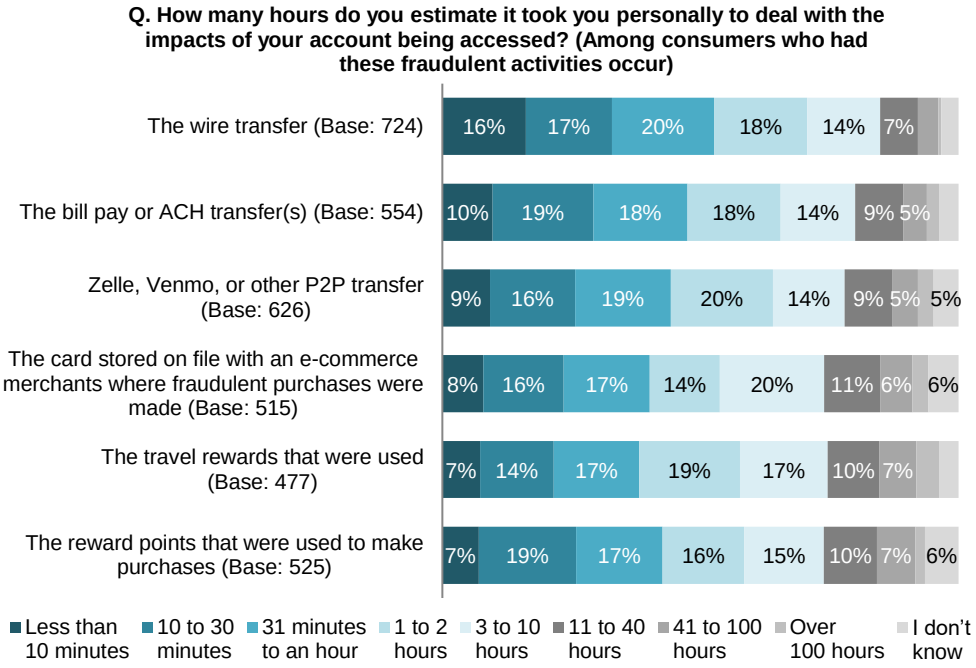


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

At least 38% of consumers who suffered a wide variety of ATO incidents were very fortunate and resolved the issue in 60 minutes or less. Unfortunately, although the percentages are quite low, every category also has consumers who spent 41 to 100 hours resolving their ATO issue and another very low percentage of consumers who spent over 100 hours resolving it (Figure 31). These are the types of cases everyone fears—being victimized and spending many hours to clear up the identity theft.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 31: Hours Required to Resolve ATO Incidents

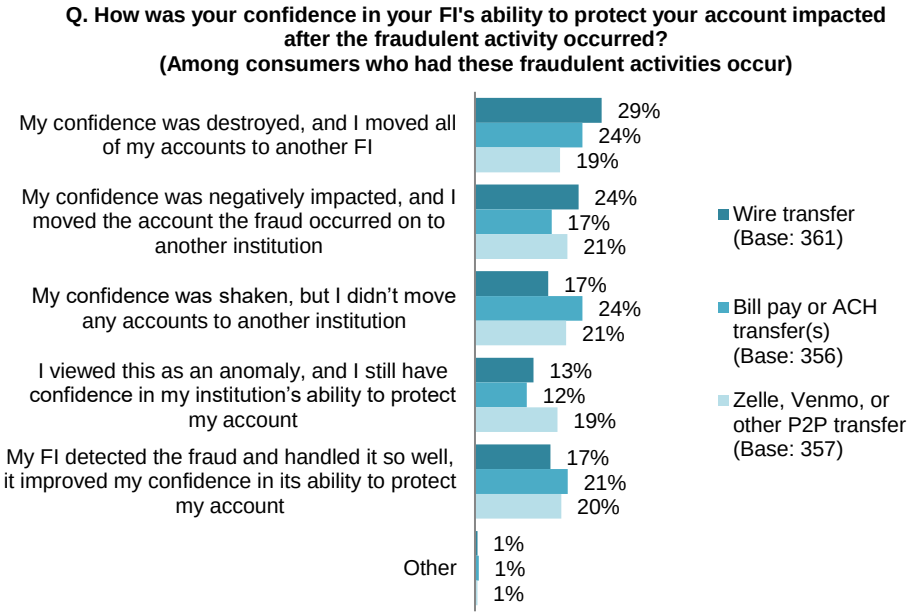


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Unlike having their PII used to open a new account or apply for benefits at an institution they may never have done business with, ATO identity theft victims were impacted by fraud on existing accounts at their own FI—the FI they had chosen to protect their money—and lost confidence in their own FI's ability to protect them. Among those whose account was taken over and a wire was used to move funds out of it, 29% stated they lost confidence in their FI and moved their banking relationship. An additional 24% also lost confidence, but just moved the account the fraud occurred on to another FI (Figure 32). A smaller percentage of consumers whose money was moved via a P2P transfer behaved similarly; attrition due to wire transfers is likely higher because larger amounts of money can be moved using that payment system than with P2P transfers.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 32: Impact of ATO on Customer Confidence in Their FI

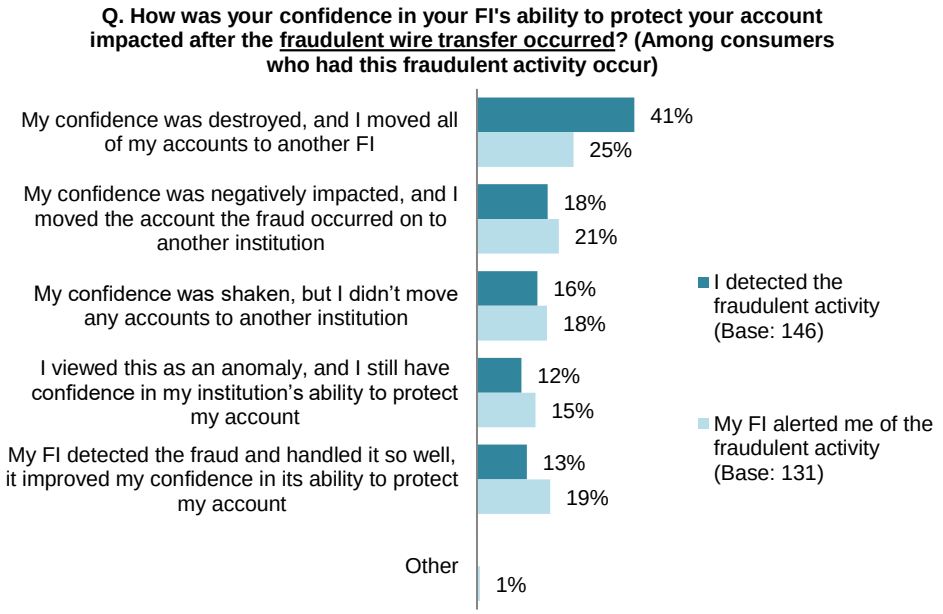


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Using wire transfers as an example, it is important to note that consumer confidence in the FI after an ATO incident is significantly affected by who detected the fraud. If the FI detected the fraud, attrition rates are much lower (46%) than if the account holder (59%) detected the fraud (Figure 33). This demonstrates the importance of strong fraud prevention efforts; even if the FI didn't prevent the fraud, the institution has a better chance of retaining the customer by detecting the fraud and dealing with it proactively.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 33: Confidence Level in the FI After a Fraudulent Wire Transfer



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

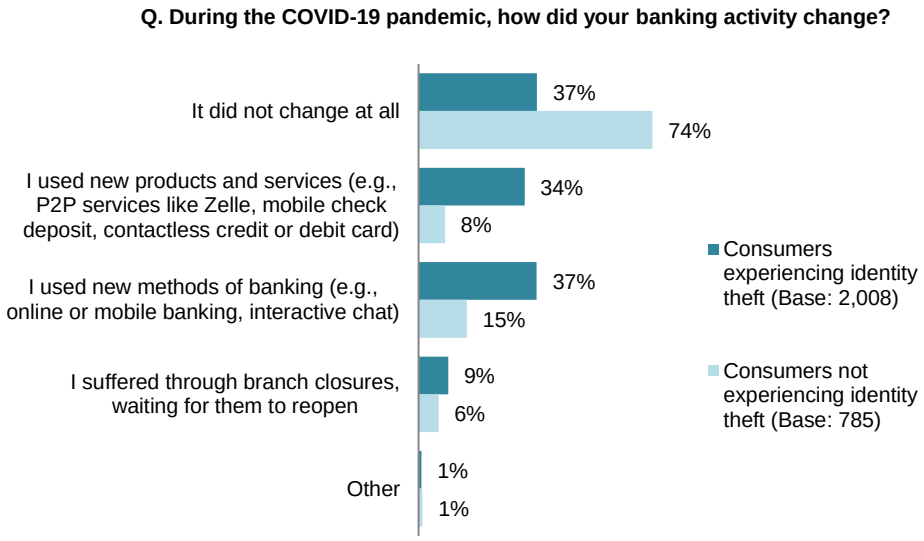
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACTS OF THE COVID-19 PANDEMIC ON BANKING

The year 2020 was unlike any most people have ever experienced, and the pandemic had a profound impact on banking. Americans have lagged behind most of the world in moving to EMV, adopting real-time payments, and becoming a digital-banking society. The pandemic forced many consumers to use new banking products and delivery channels for the first time due to branch closures that lasted for weeks or months. People had to have access to their money to survive, so call centers were flooded with people seeking assistance, and many were forced to learn new methods.

Even in light of all of the branch closures and upheaval, 74% of consumers who did not experience identity theft fraud in 2020 stated their banking behavior was not impacted at all by the pandemic. Eight percent of those who did not experience identity theft fraud tried new products, and 15% tried new methods of banking. Clearly, consumers who experienced identity theft were more willing to try new things, as 34% of those who experienced identity theft tried new products and services and 37% tried new delivery channels (Figure 34). Were these digital newbies more susceptible to fraud because they were new to these products or channels? Clearly, fraudsters were very active in 2020 executing various consumer scams (e.g., imposter scams, romance scams) at higher rates than ever before,[6] so some of these consumers may have been victims of some of the scams.

Figure 34: Banking Activity Changes Due to the Pandemic



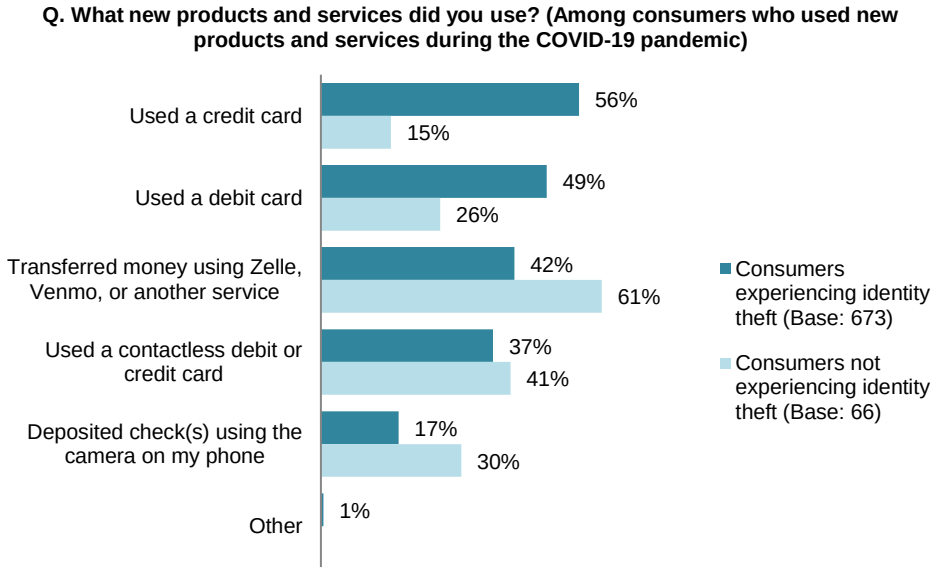
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

6. Monica Vaca, "The Top Frauds of 2020," FTC Consumer Information, February 2, 2021, accessed February 10, 2021, https://www.consumer.ftc.gov/blog/2021/02/top-frauds-2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Consumers used a variety of banking products that were new to them during the pandemic. Some consumers used a credit card or debit card for the first time, while others used a contactless version of those cards for the first time. Some consumers used a P2P payment such as Zelle or Venmo for the first time, and some deposited a check into their account using the camera on their phone for the first time. Unfortunately, many consumers who used these products and services for the first time (particularly credit cards and debit cards) also experienced identity theft in the past two years (Figure 35).

Figure 35: New Products and Services Used During the Pandemic

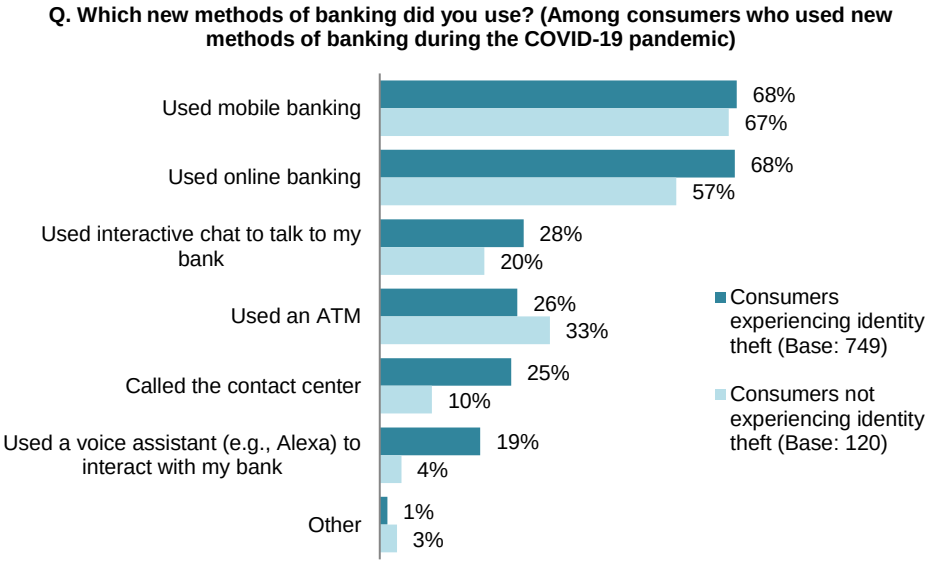


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Many consumers also used new methods of banking in 2020; the bulk of consumers who did so used online or mobile banking for the first time. Other new methods of banking included using an ATM for the first time, calling the contact center, or using chat or a virtual assistant to communicate with their FI. The percentage of consumers who tried these new methods of banking were similar in most cases between those who did or did not experience identity theft. The exceptions are those calling a contact center for the first time or using a voice assistant to do banking; in those groups, higher percentages experienced identity theft than not (Figure 36).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 36: New Methods of Banking Used During the Pandemic

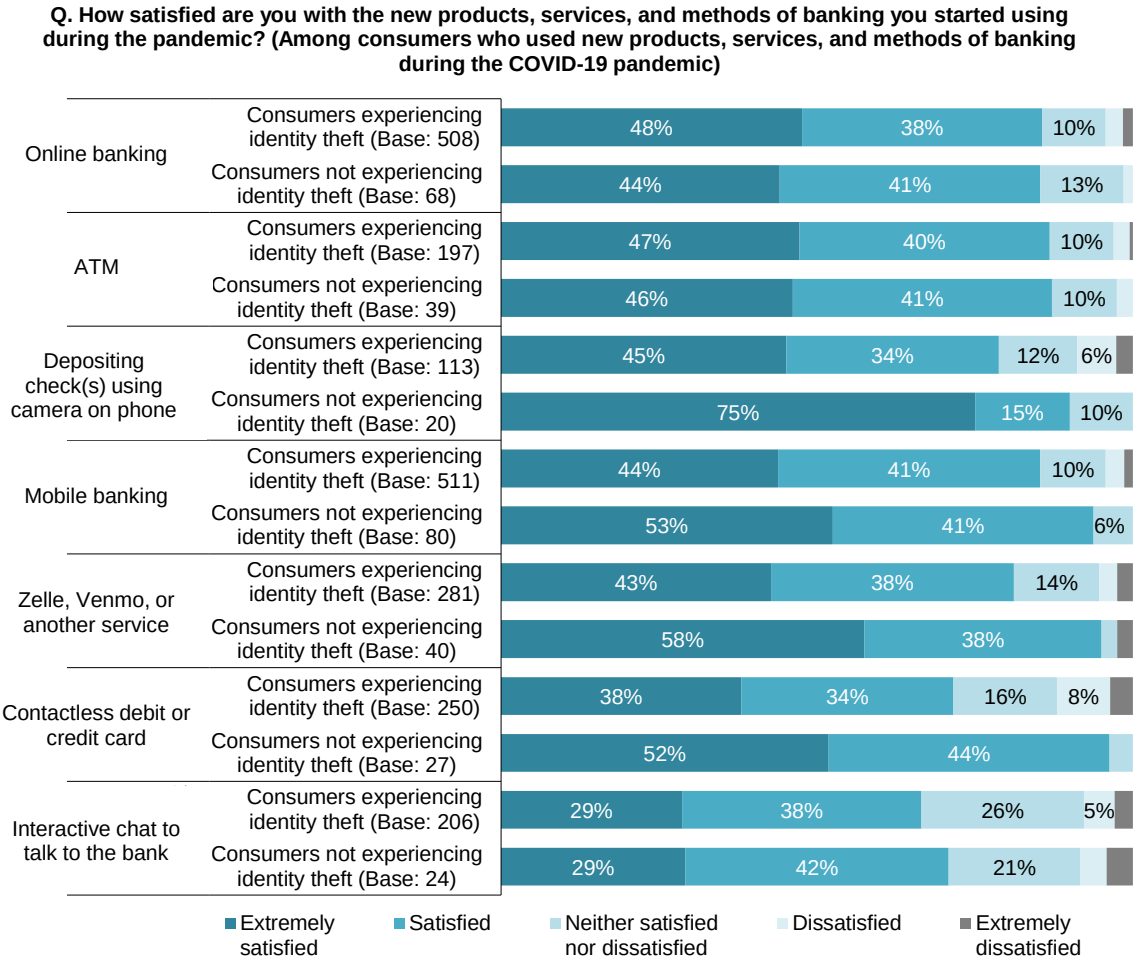


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

The good news is that a large majority of consumers who used new products, services, or delivery channels in 2020 were satisfied with these new experiences. The lowest percentage of any category involved identity theft victims who used interactive chat to talk with their bank; only 67% of those consumers were satisfied with the new method. At least 85% of consumers who used online or mobile banking for the first time were satisfied. The percentages of consumers who were dissatisfied with the new methods of banking they used were very low (Figure 37).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 37: Satisfaction Levels With New Products, Services, and Methods of Banking



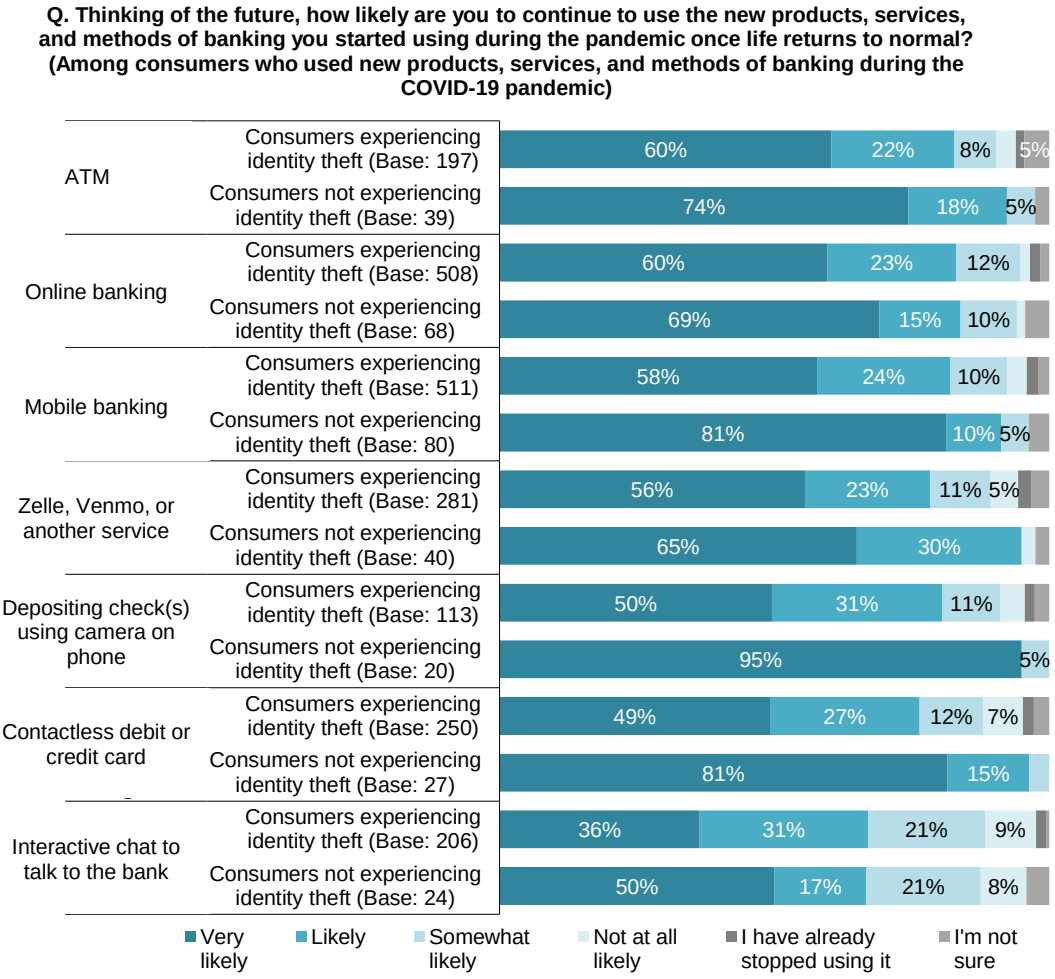
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

The very best news for FIs is that the majority of consumers who tried new banking products and services or delivery channels in 2020 are likely to continue using them. At least 82% of consumers who used online or mobile banking for the first time in 2020 plan to continue to use the new delivery channel in the future. While there are some people who are not likely to continue using the new capabilities tried in 2020, or have already stopped using the new capabilities, these percentages are quite small. Consumers who experienced identity theft are more likely to discontinue using mobile banking (or have already stopped using it) than are consumers who did not experience identity theft (Figure 38).

This move to using digital products, services, and channels is much more cost-effective for FIs. While the pandemic is a terrible thing to endure, at least this silver lining is a welcome one.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 38: Likelihood of Continuing to Use New Banking Products, Services, and Methods

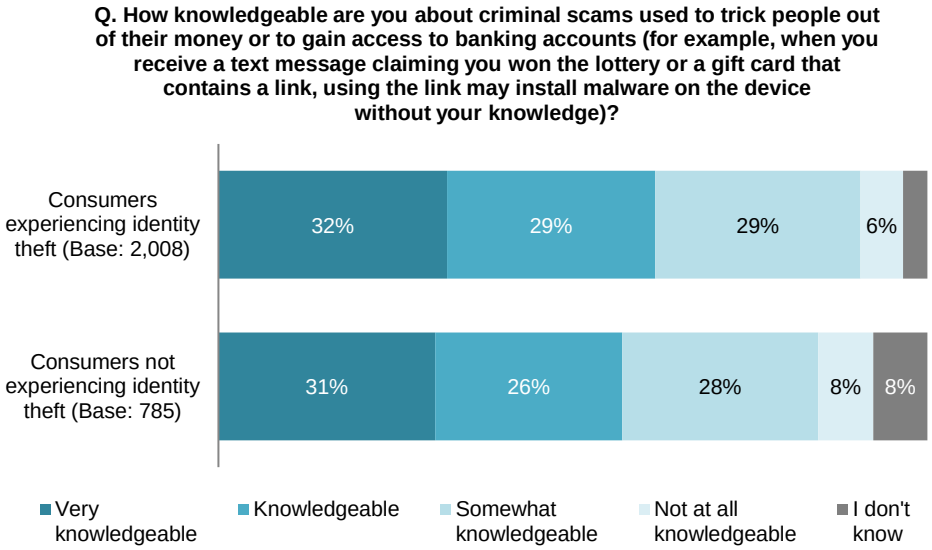


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Very similar percentages of consumers believe they are knowledgeable about fraud scams whether they experienced identity theft (61%) in the past two years or not (57%). An additional 29% or 28%, respectively, deem themselves somewhat knowledgeable (Figure 39). Given the tremendous number of digital newbies, it is imperative that people receive education about how to best protect themselves proactively and how to recover if they are victimized. Nobody is capable of knowing what they do not know, and fraudsters have demonstrated many times how creative they can be.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 39: Knowledge of Criminal Scams



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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RECOMMENDATIONS

FIs have many opportunities to prevent fraud and retain customers. It can be very difficult to protect them against family and friendly fraud. Identity theft is insidious, and in many cases, is committed by those close to the individual. Here are some recommendations for best dealing with identity theft and planning to assist all the digital newbies in your customer base.

Identity theft:

- Be proactive in upgrading current methods of authenticating applicants and returning customers. Most consumers' PII has been breached and is available to fraudsters, so doing the same things done in the past is no longer enough.
- Consider using physical and behavioral biometrics, digital identities that include device recognition, geofencing, and other new technologies that help authenticate consumers more reliably than passwords, knowledge-based questions, and third-party databases.
- Develop procedures to better assist individuals who dispute new accounts opened at your FI. If these are identity theft victims, and they are treated like criminals, they are unlikely to ever do business again with your FI in the future.
- Have strong fraud prevention and detection systems in place. Some attrition will occur after ATO attacks because consumers will have lost confidence in your FI's ability to protect their accounts. Attrition can be decreased if the FI detects the ATO and proactively tries to recoup funds and contact the customer.
- Analyze the fraud impacting your FI to determine whether adjustments to your authentication procedures can be made to proactively identify and stop fraudulent applications or activity.

Post-pandemic banking:

- Educate customers (especially digital newbies) about scams, family and friendly fraud, elder abuse, and other issues so they become knowledgeable and can avoid being victims to the extent possible.
- Ensure your FI provides a way for consumers who have questions to learn more about scams and other fraud-related issues.
- For consumers who revert to pre-pandemic banking methods, try to learn why they were not happy using new products and services they used during the pandemic. A bit of education may help them be more comfortable using them again.
- Listen to common customer questions and develop a FAQ to share with all customers. Questions that are asked by several people are likely to be ones many others are wondering about but may never ask.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

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

Top 10 Trends in Fraud & AML: Onward and Upward, January 2021.

Key Trends Driving Fraud Transformation in 2021 and Beyond, December 2020.

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

Beating the Bad Guys: Safe and Secure Voice Interactions in the IVR, November 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Shirley Inscoe
+1.617.398.5050
sinscoe@aitegroup.com

Research Design & Data:

Sarah Fitzsimmons
+1.617.398.5039
sfitzsimmons@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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com