Early Warning®

Aite Novarica

PLAYING LEAP FROG WITH THE BAD GUYS: A HOLISTIC BLUEPRINT TO KEEP YOU ONE HOP AHEAD

September 2021

Panelists

- Moderator -

Robin Love

Vice President, Product Management
Early Warning®

- Presenter -

Shirley Inscoe

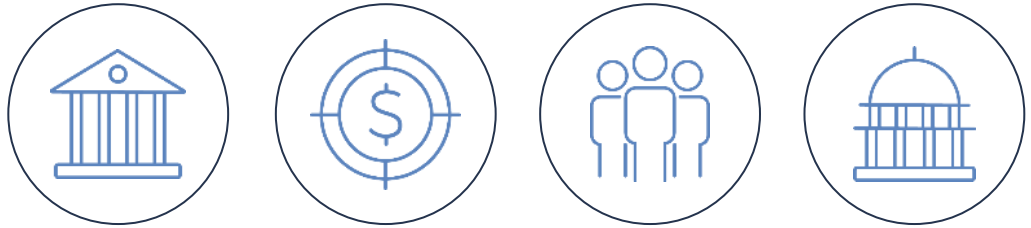
Strategic Advisor, Fraud & AML Practice
Aite-Novarica Group

Early Warning®

BANK-OWNED, PRIVATELY HELD FINTECH, FOUNDED IN 1990

OUR CUSTOMERS

Early Warning® serves **45 of the top 50** financial services companies and **over 3,500** business customers directly and indirectly, including financial institutions, government agencies and payment companies.



BANKS & CREDIT UNIONS | **RESELLERS** | **CONSUMERS (P2P NETWORK)** | **GOVERNMENT AGENCIES**

Equal ownership by seven of the nation's largest financial institutions

TRUIST | WELLS FARGO | Capital One | PNC | BANK OF AMERICA | usbank | JPMorganChase

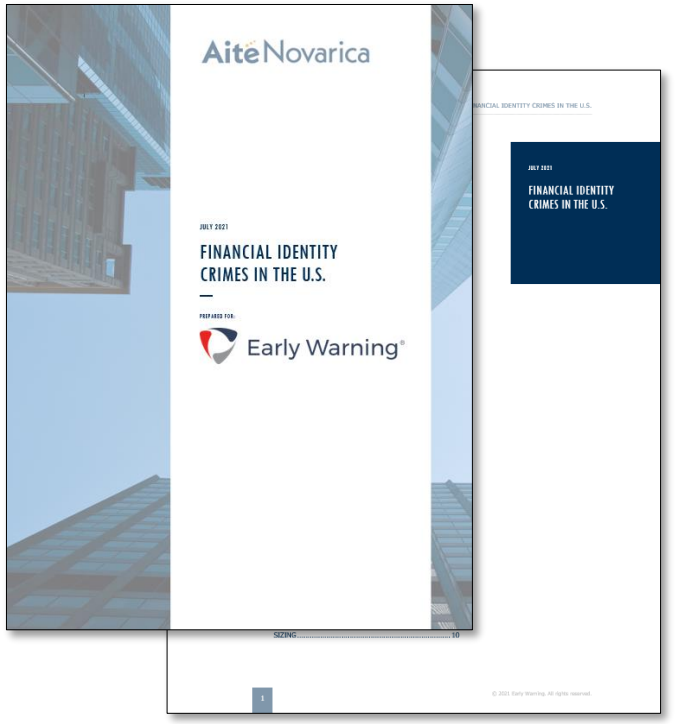
The increasing nature of fraud

- Consumers want a secure, frictionless financial experience

43% of U.S. consumers experienced financial identity theft (application fraud in their name or account takeover [ATO]) in the past two years[1]

Less than half of consumers or 43% of respondents in an Arizent study have faith in financial service providers to protect their data privacy[2]

- To meet today's challenges and protect the future, financial institutions (FIs) need to update their fraud mitigation solutions.



Financial Identity Crimes in the U.S.
Commissioned by Early Warning® and produced by Aite-Novarica Group

Sources:

1. Financial Identity Crimes in the U.S. Aite-Novarica Group. August 2021
2. Data Privacy and Security 2021: Fear, Malaise and Eroding Trust. Arizent, 2021

Presentation

SHIRLEY INSCOE, STRATEGIC ADVISOR, AITE-NOVARICA GROUP

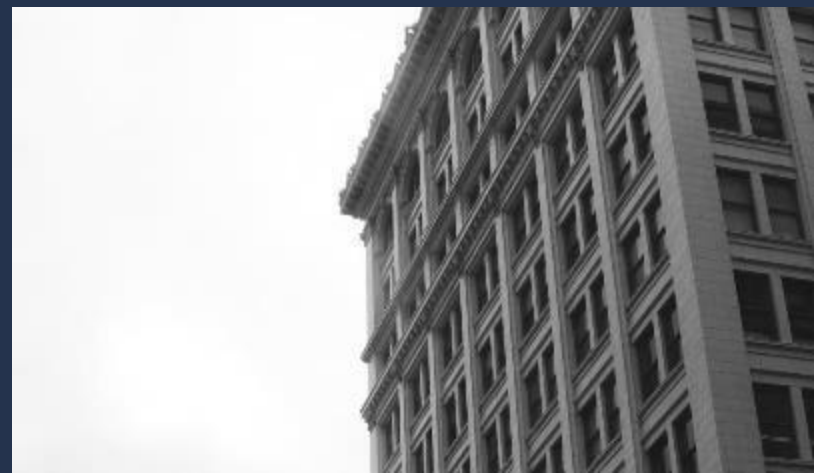
sinscoe@aitegroup.com | +1.617.398.5050 | www.aite-novarica.com

Early Warning®

About Aite-Novarica Group

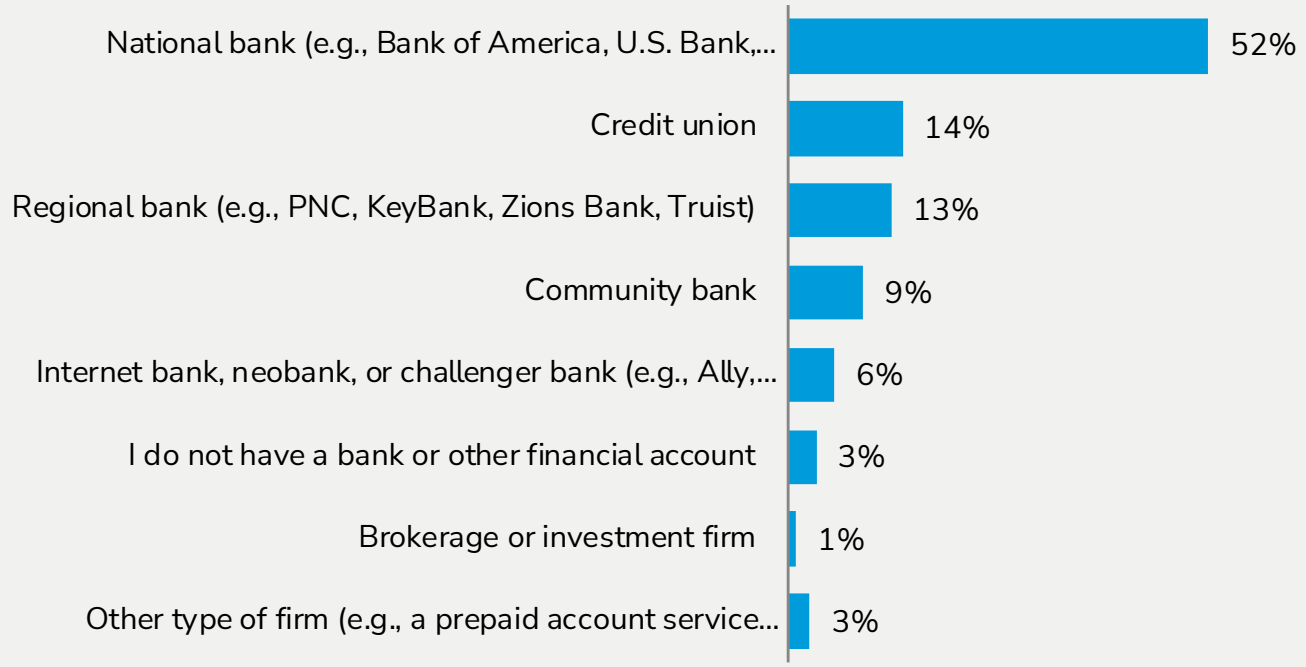
Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, 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.

Visit Aite-Novarica Group on the web and connect with them on Twitter and LinkedIn.



Consumers participating in this research

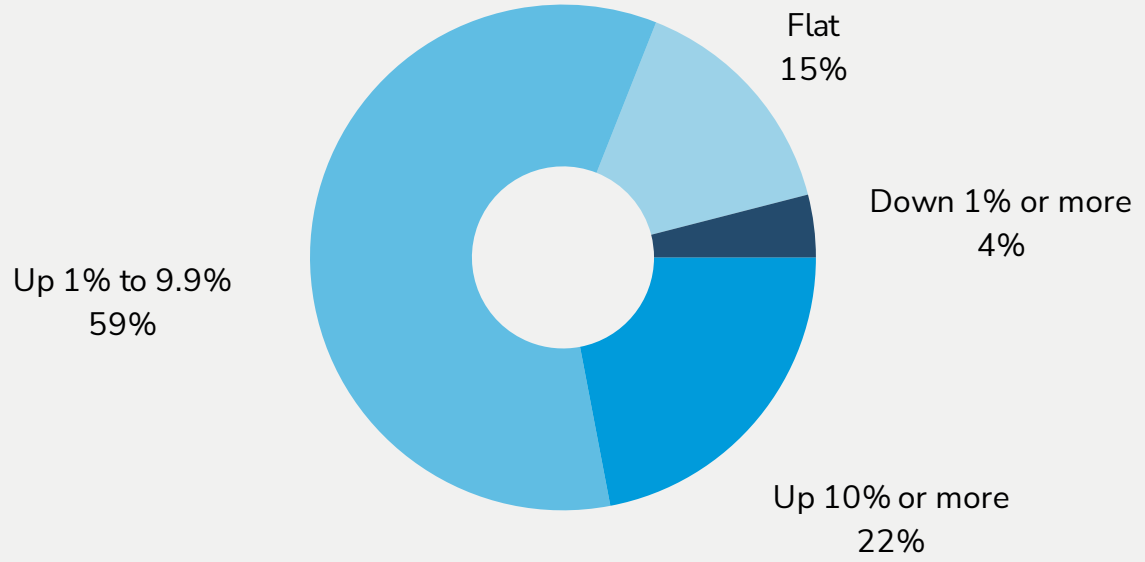
Q. Which of the following do you consider to be the primary bank or financial services provider that you use to manage most of your day-to-day finances? (Base: 8,653 consumers)



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

Application fraud trend

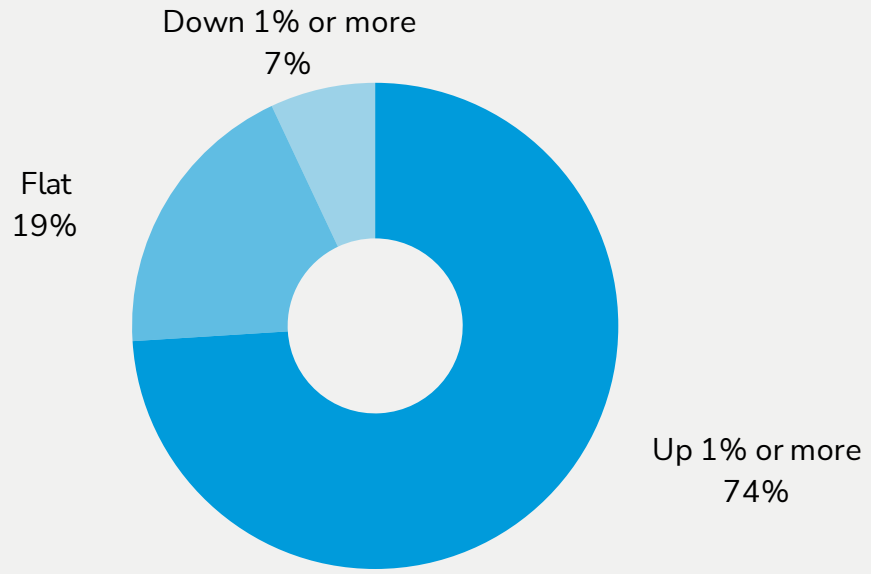
Q. Please indicate the trend associated with application fraud, comparing attack rates today to attack rates prior to the pandemic.
(n=27)



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

Synthetic identity fraud trend

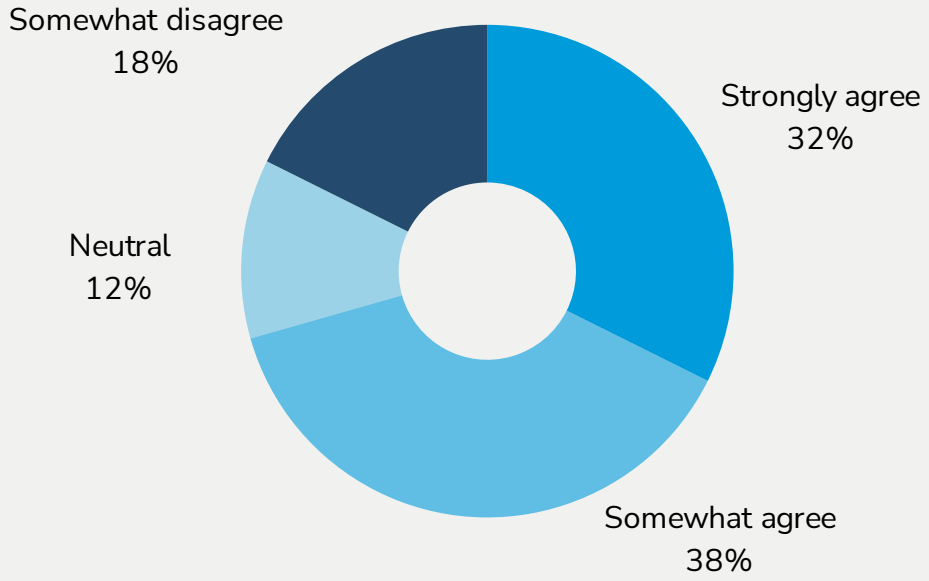
Q. Please indicate the trend associated with synthetic identity fraud, comparing attack rates today to attack rates prior to the pandemic. (n=27)



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

Synthetic identity challenge

Q. To what extent do you agree with the following statement: "Synthetic identities are a bigger challenge than identity theft"? (n=34)



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

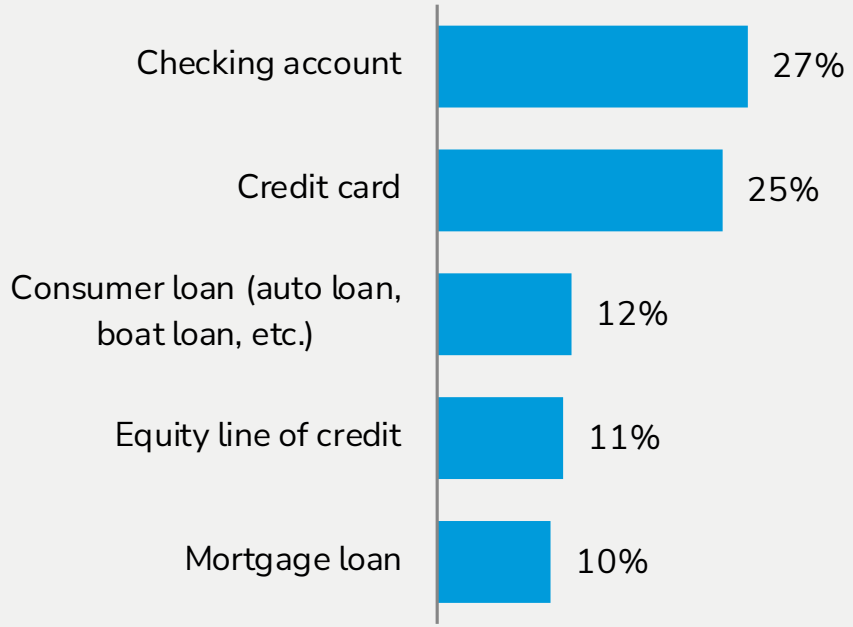
Identity theft via application fraud

Consumers Experiencing Any Type of Application Fraud in Financial Accounts
(Base: 8,653 consumers)

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

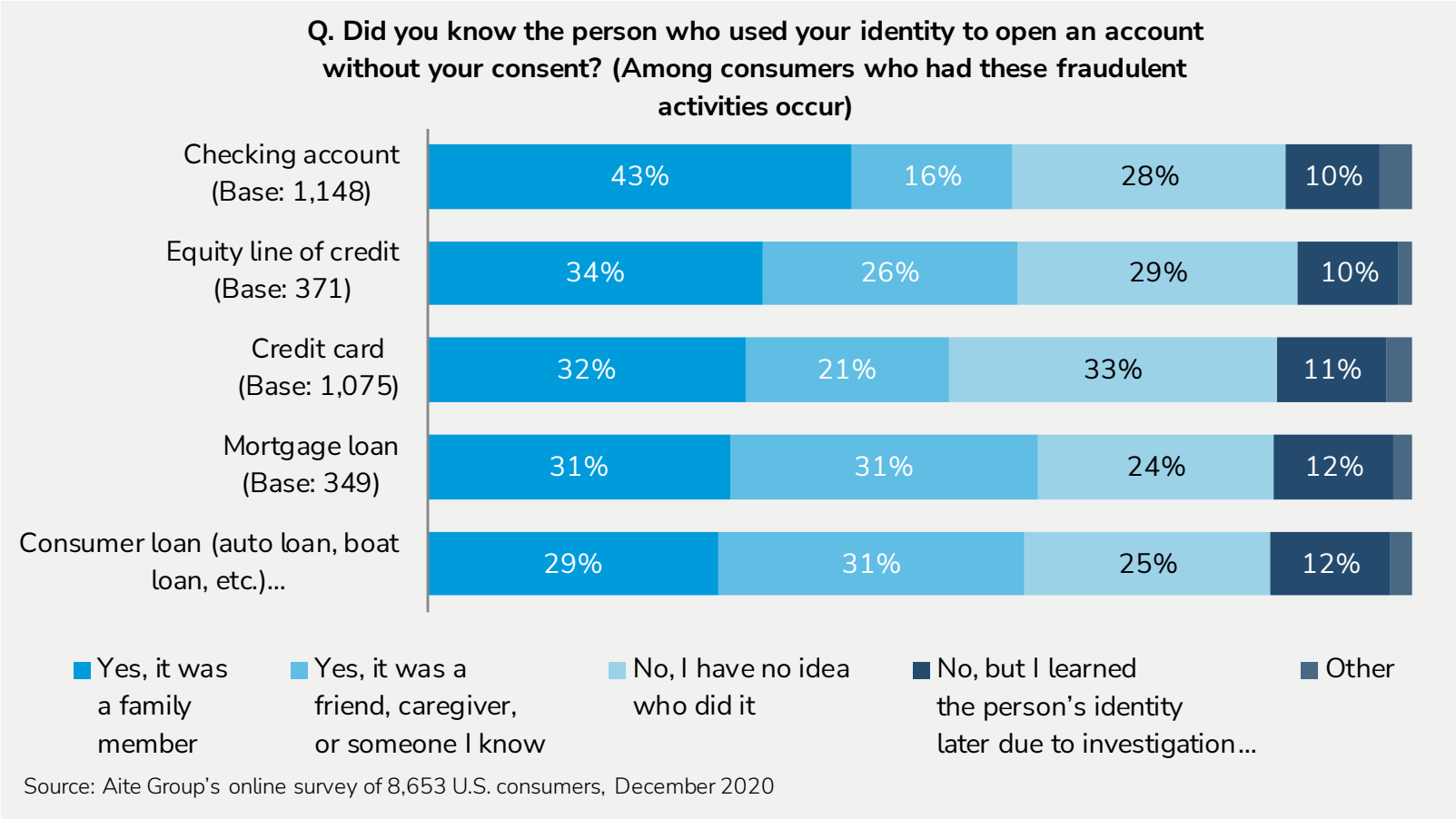
Common application fraud types

Q. During the past two years, has your personal information been used without your consent to open any of the following accounts 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

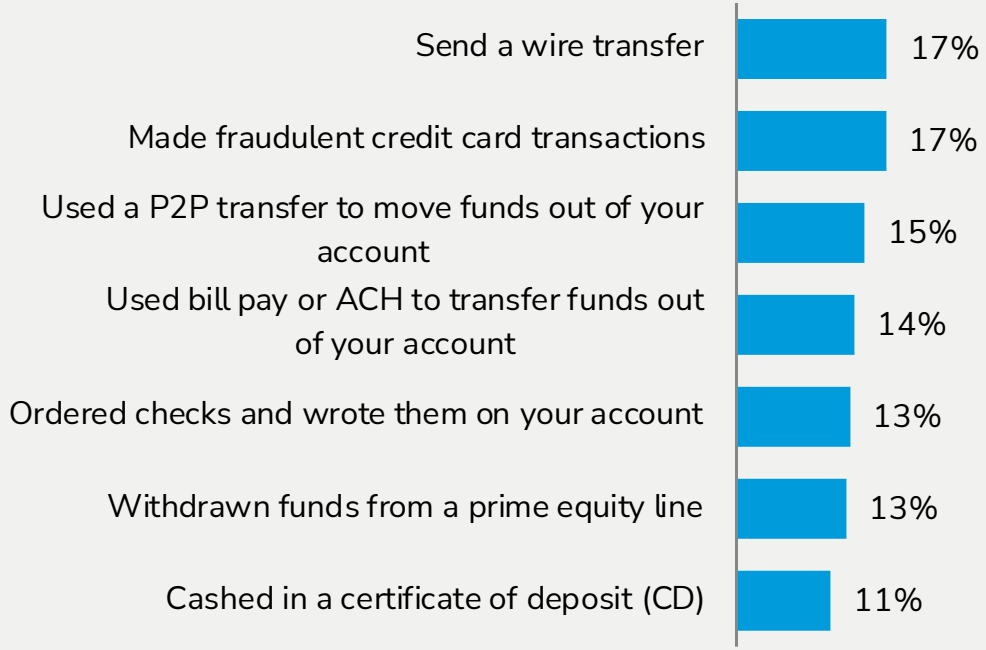
Family and friendly fraud



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

Identity theft via account takeover

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: 8,653 consumers)

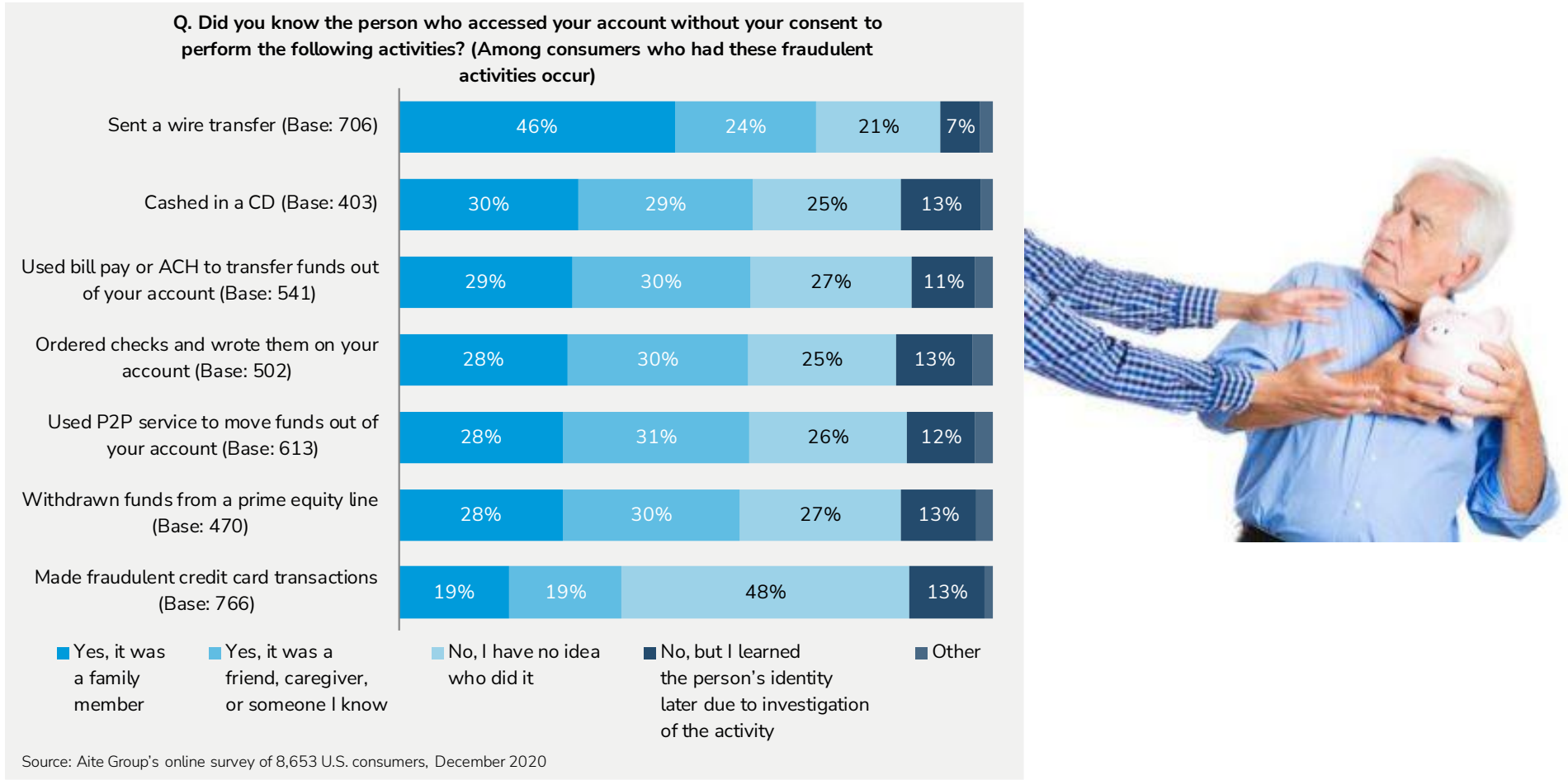


Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Sophistication of fraud attacks and scams

- Increasingly sophisticated attacks
- Tailored attacks
- Scam rates at an all-time high
  - Advance fee fraud, romance scams, lottery scams, employment scams
- Digital newbies may be more likely to fall for scams
  - Millions turned to online and mobile banking during pandemic
- All payment systems are at risk of use for fraud

Family and friendly ATO fraud



Recommendations

- Proactively assess and upgrade the 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. They will likely tell their friends about the poor treatment they feel they received, somewhat tarnishing the reputation of the FI.

Recommendations continued

- 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 identify and stop fraudulent applications or activity.
- Apply a multipronged detection capability. Use many sources of data (e.g., credit bureaus, third-party databases, and employment and income verification) to try to detect both identity theft and the use of synthetic identities. There are no silver bullets in fighting fraud, and layers of protection will enable the greatest success in preventing identity crimes.

Discussion

MODERATED BY ROBIN LOVE, VICE PRESIDENT, PRODUCT MANAGEMENT, EARLY WARNING®

Early Warning®

In your opinion, do you think financial institutions are committed to permanent changes in technology and security as a result of the changing fraud landscape?

Why should financial institutions address today's fraud challenges with an end-to-end approach?

What are some of the best practices on how to balance a customer's experience while mitigating risks?

Questions?

Contact:

WWW.EARLYWARNING.COM/ID

marketing@earlywarning.com

Early Warning®