Arkose Labs

Q1 FRAUD REPORT

FOCUS ON FINANCIAL SERVICES

Introduction

Like all industries, financial services dealt with massive increases in digital usage during 2020, which in turn led to spikes in fraud as well. As homebound people the world over went online for shopping, entertainment, education, socializing, remote work and more, this led to an increase in attacks as fraudsters attempted to blend in with good users. With more people online at all hours of the day, typical models of what good and bad behavior looked like were thrown out the window.

In the financial space, fraudsters targeted government relief packages that flowed through financial institutions, as well as fraudulently applying for loans and lines of credit. This has created a booming business around pandemic-related fraud, one that has caused billions in losses already. As many banks have invested in digitizing their entire customer relationship, this has in some cases unwittingly created security loopholes, attracting fraudsters who are committing a wide range of abuses including identity theft, fake account creation and first-party fraud before it can be detected. This is likely to cause further grief for financial services as regulators will take an increasingly hard line on lax security measures.

No one knows what the rest of 2021 holds, but it's imperative we all work together to stamp out fraud and make the digital world a safer place for all. Though we may be turning the page on 2020, one thing that is certain is that the frequency and severity of fraud attacks will never go back to pre-pandemic levels.

2020 In Review: Financial Services

660,000
SWEATSHOP ATTACKS

2.46 Million
BOT ATTACKS

3.13 Million
TOTAL ATTACKS

87 Million
TOTAL TRANSACTIONS

3.61%
ATTACK RATE

21.4%
HUMAN ATTACKS

VS

78.6%
BOTS ATTACKS

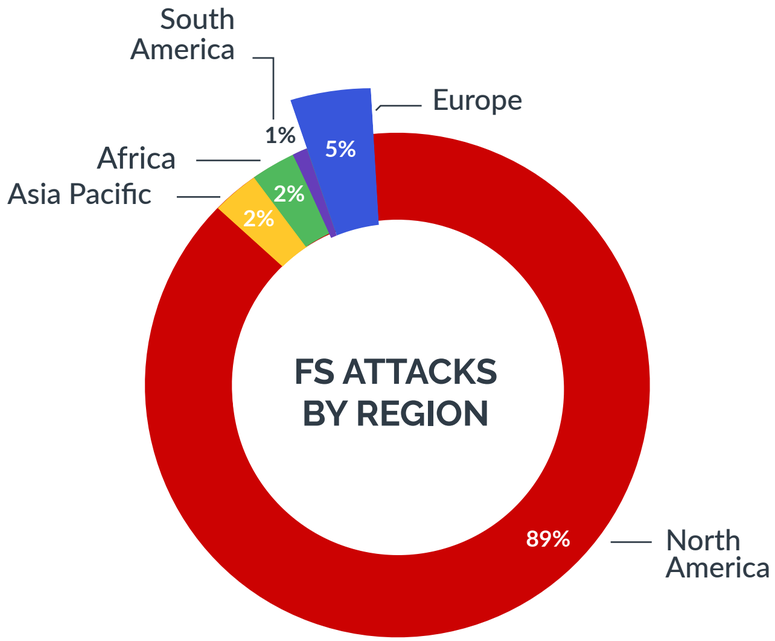
52.2%
DESKTOP ATTACK RATE

VS

47.8%
MOBILE ATTACK RATE

2020 Attacks By Region

2020 saw marked change in the geographies where fraud attacks originate from. Typically, the majority of fraud attacks are launched from countries with developing economies, where employment opportunities may be low. These are typically fertile grounds for fraudsters to recruit from. However, as the Covid-19 pandemic pushed millions around the world into financial despair, many resorted to fraud out of desperation to make ends meet. As you can see, the vast majority of financial services attacks came from North America. This was largely influenced by attacks originating from the United States, where tens of millions of people were suddenly thrown into unemployment and financial distress due to Covid-19 lockdowns.



What Changed in 2020 for Financial Services?

LOAN FRAUD RAMPANT

Lockdowns suddenly plunged many into financial distress, and consumers rushed to financial institutions to take out emergency loans. At the same time, business owners also sought loans and access to government programs such as the PPP to stay afloat. Fraudsters took advantage of this mass demand, applying for fraudulent personal and business loans as FI's systems faced high demand.

INCREASED FRIENDLY FRAUD

Many normally "good" customers were pushed to commit acts of fraud they normally would not have due to financial distress. Banks saw a marked rise in so-called "double-dipping" where a consumer orders a product, and then goes back to their bank and claim the order was fraudulent or that they never actually placed it. Some also put stimulus money on a payment mechanism, spent it and then claimed they never made the transaction.

THE RISE OF DIGITAL PAYMENTS

Many have been predicting a cashless world for years, and while adoption of digital payments has steadily increased in recent years, 2020 finally saw a massive increase in digital payments usage. Out of necessity, consumers flocked to digital payments platforms to transact online. Even those who shopped in-store during the pandemic relied heavily on contactless digital payments as opposed to handling cash.

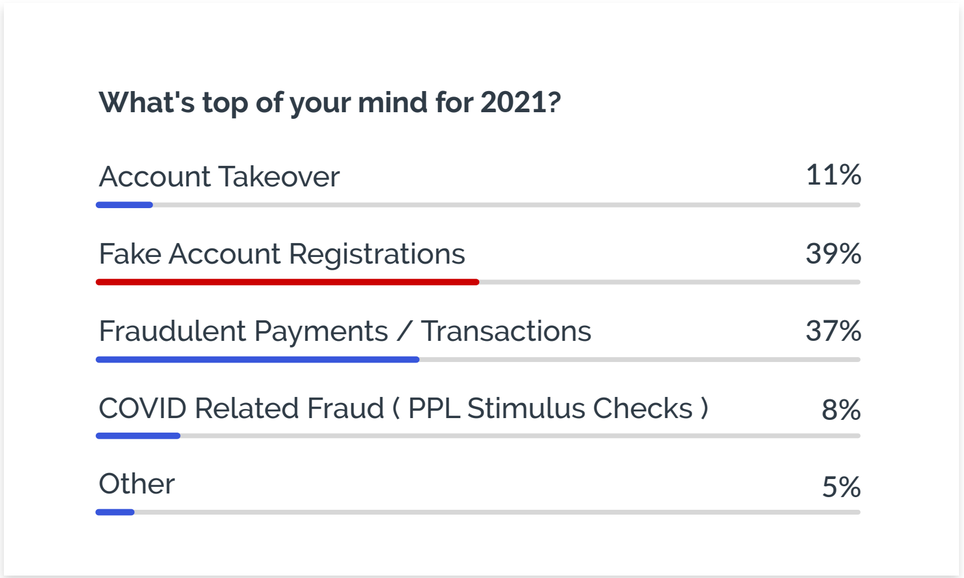
A STRESS TEST OF FRAUD SYSTEMS

The massive spike in digital traffic to online platforms, and the correspondent spike in fraud attacks, made for something of an unexpected stress test for financial institutions' fraud systems. Suddenly, old models of what suspicious behavior looked like were thrown out the window, and for many platforms daily traffic was at rates normally only reserved for the busiest times of year.

Fintech Survey: 70% of Businesses Saw Increased Fraud Attempts in 2020

Arkose Labs surveyed 100 fraud and security professionals at fintechs and financial institutions. One quarter of all execs surveyed reported a "major increase" in fraud and abuse attempts in 2020, with a further 44% saying they had seen a slight increase. This rise reflects not only an increasingly hostile threat landscape in general, but the fact that fast-growth, digital-first financial companies are juicy targets for attackers.

It is interesting to note that while Covid-19 related threats such as Payroll Protection Program (PPP) and stimulus check fraud are a top topic of discussion as an emerging problem, it is actually long-standing issues such as protecting transactions and bogus fake new accounts which is most concerning for respondents.

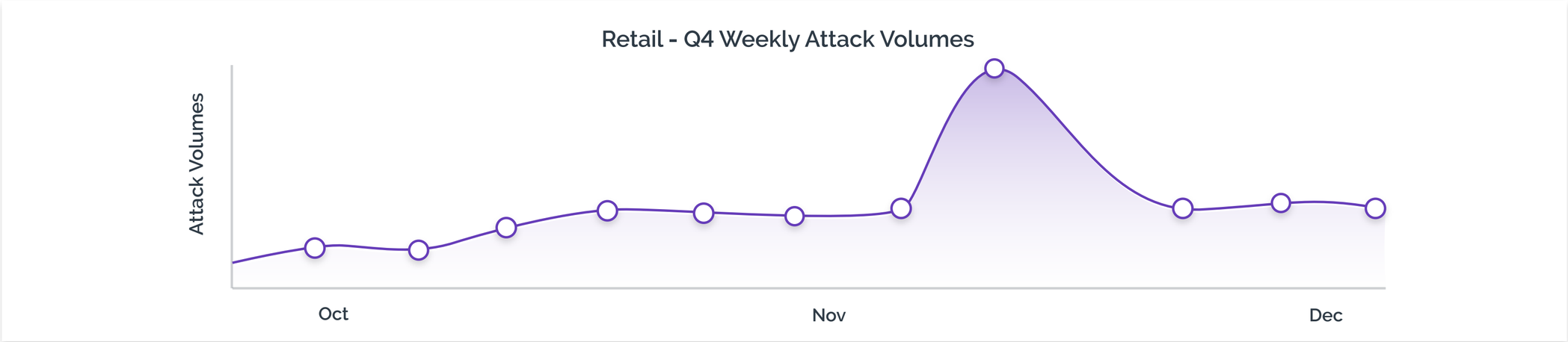


Financial Services: Fake Applications are a Chief Concern

Financial Services firms were deluged with fake credit card and personal loan applications in 2020, as well as fraudsters targeting government programs meant to help small businesses, such as the PPP.

In Q4, fraud targeting the financial services sector slowed a bit; the industry saw a 2.6% attack rate. This was mostly focused on application fraud, with the Arkose Labs Network monitoring 719,263 attacks. This means financial services firms need to continue to be vigilant about new account registration fraud.

Financial services also had the highest percentage of mobile transactions out of all industries at 57.8% This continues a years-long trend of consumers ditching physical branches and conducting their financial lives online. Mobile-centric fraud and security should be a top concern.



Case Study: A Better Digital Banking Experience

Arkose Labs worked with one of the largest global banks, which was facing frequent attacks targeting user accounts. Fraudsters used bots to power credential stuffing attacks at scale, account takeovers, and new loan and credit application fraud. The client had relied on an older, legacy solution for fraud prevention and authentication, but these were ineffective at stopping automated attacks.

- Bot attacks
- Credential Stuffing
- Account Takeover
- Application Fraud

The bank deployed Arkose Labs to stop the wave of these attacks. Taking a unique approach to fraud prevention and user authentication, the Arkose Labs platform undermines the financial incentive behind fraud, thus dissuading bad actors from even launching attacks in the first place. The Arkose Labs Fraud and Abuse Platform combines real-time intelligence, rich analytics, and adaptive step-up challenges to progressively diminish the profitability of attacks while adapting to evolving attack patterns. Arkose Labs' custom enforcement challenges are context-based, adaptive visual challenges that will thwart large-scale account takeover attempts.

The Arkose Labs Fraud & Abuse platform allowed the bank to drastically slash the number of successful attacks, protect genuine users, and ensure a safe digital banking experience for all customers. Furthermore, a dedicated managed services team works with every Arkose Labs client to ensure the platform is always fine-tuned to deal with the latest evolving threats. Arkose Labs regularly provides custom insights to the bank, allowing it to adapt and alter its own internal fraud controls as needed.

Financial Services: The Target of Downstream Fraud and Abuse

Even when not directly targeted by fraud themselves, financial services companies and their customers can still be at risk from attacks on other touchpoints.

For example, Interpol in January issued a notice describing a new fraud scam targeting users of dating apps to promote fake investments.[1] As part of the scam, fraudsters created fake new accounts and matched with genuine users. After a few messages had been exchanged and a level of trust had been established, the fraudster then begins giving the victim investment "tips" and lure them to download a fake trading app, link a bank or payments account to it, and sign up for financial products. Once the match has been milked for their cash, victims are locked out of their fake 'investment' accounts and the scam artist vanishes. Overall. Arkose Labs detected four million online dating fraud & abuse-related attacks in 2020.

All social engineering scams are created to drive confidence and trust with the victims. These fraudsters are well trained in how to approach them. Especially amid Covid, consumers are in a vulnerable time as many are lonely and are looking for connection on the internet. Often, as in the case above, the ultimate target is the victim's banks account or other financial information. This means financial institutions must be especially vigilant about monitoring activity in customer accounts, such as transactions and payments, in order to stop

[1]https://www.zdnet.com/article/interpol-warns-of-romance-scam-artists-using-dating-apps-to-sign-victims-up-to-fake-investment-schemes/

Conclusion

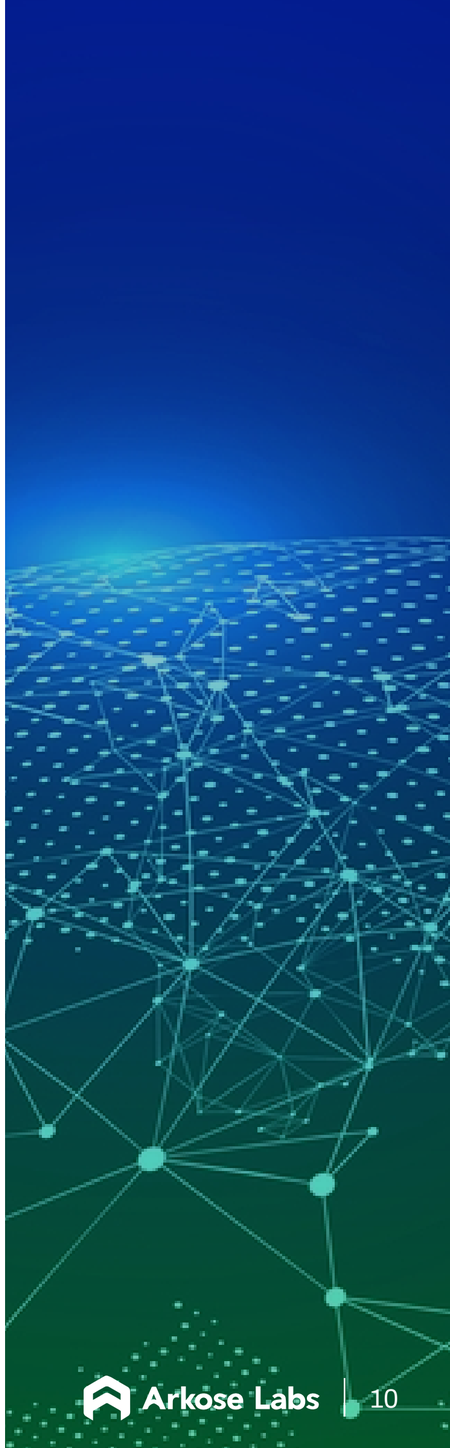
Fraud attacks became more frequent and more severe once the world was plunged into lockdowns related to the Covid-19 global pandemic. And as we ease back into something more resembling normal, don't expect fraud to return to previous levels along with it.

Financial institutions and fintechs will always be a high target for fraudsters due to the extremely valuable customer data they hold

That means financial services companies should expect to continue to see the high levels of credential stuffing that occurred in 2020 to continue, as attackers test stolen credentials to repeatedly launch ATO attacks. Account takeovers of financial accounts are so critical to fraud not just because money can be drained or payments credentials stolen, but because fraudsters then use those to fund a range of further attacks.

As waves of new adopters continue to access digital financial services -- many for the first time -- preventing these attacks on customer accounts will be critical. As a highly regulated industry as well, financial firms face fines and regulatory scrutiny if customer accounts are compromised at scale.

Fighting fraud may be more complicated than ever, but with the right approach and the right tools, we can stop the bad guys in their tracks while still maintaining a great digital experience for customers.



About Arkose Labs

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales: (800) 604-3319

Offices

San Francisco
250 Montgomery St 10th Floor, San

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo