EBOOK

FIVERITY

WOLF & COMPANY, P.C.

The Fraud & Compliance Crises Facing Challenger Banks

How Digital Banks Can Seize Online Growth While Navigating the Impending Fraud Crisis

November 2022

Table of Contents

03 Introduction

04 The Digital Banking & Fraud Landscape

04 Shift to Online

05 Challenger Bank Market Opportunity

07 Accelerated Growth

08 Rise in Fraud

12 Challenger Bank Regulatory & Compliance Issues

14 Neobanks: Ideal Targets for Fraud

14 Why Are Digital Banks Susceptible to Fraud?

17 Who Targets Digital Banks?

18 Types of Fraud Facing Digital Banks

23 Broader Money Laundering and Human Trafficking/Smuggling Concerns

25 Impact of Money Laundering & Fraud

27 Fighting Back

30 BSA/AML/OFAC & Fraud Risk Assessment

31 Conclusion

Introduction

The growth of digital banking in the U.S. has largely followed smartphone penetration.

- Mid 1990s: Traditional banks experiment with digital banking services.
- 2010: Smartphone penetration reaches a critical mass and investors begin funding the first generation of fully digital (aka, "challenger") banks.
- Digital banking is given a boost by the pandemic.
- Digital banks gain a competitive edge by adopting a mobile-centric user experience and catering to younger consumers and niche markets.

> In consumer banking, you have what is one of the largest industries in the United States, in terms of profits, and at the same time one of the least disrupted industries, and the most unpopular with consumers. Those three things create a perfect storm for disruption."
>
> Andrei Cherny / CEO / Aspiration

In their short history however, digital banks have experienced extremely high rates of fraud and numerous compliance issues.

- With companies like PayPal[1] discovering millions of illegitimate accounts, analysts question how much of the digital bank segment's new customer accounts are driven by similarly driven by fraud.

Impending fraud crisis: As sophisticated fraudsters nurture their accounts over time to build up credit worthiness for a costly "bust-out," it could take up to two years for the extent of fraudulent accounts within digital banks to be fully understood.

Compliance issues include:

- Lax fraud, BSA/AML and OFAC sanctions, and AML processes and controls.
- Issues stemming from the "rent-a-charter" model has led to consumer confusion as to whether their digital bank is actually a bank.

[1] Sifted, February 8, 2022. "Digital Banks Biggest Challenge Isn't Growth. It's Fraud." https://sifted.eu/articles/fraud-digital banks-challenge-fintech-paypal/

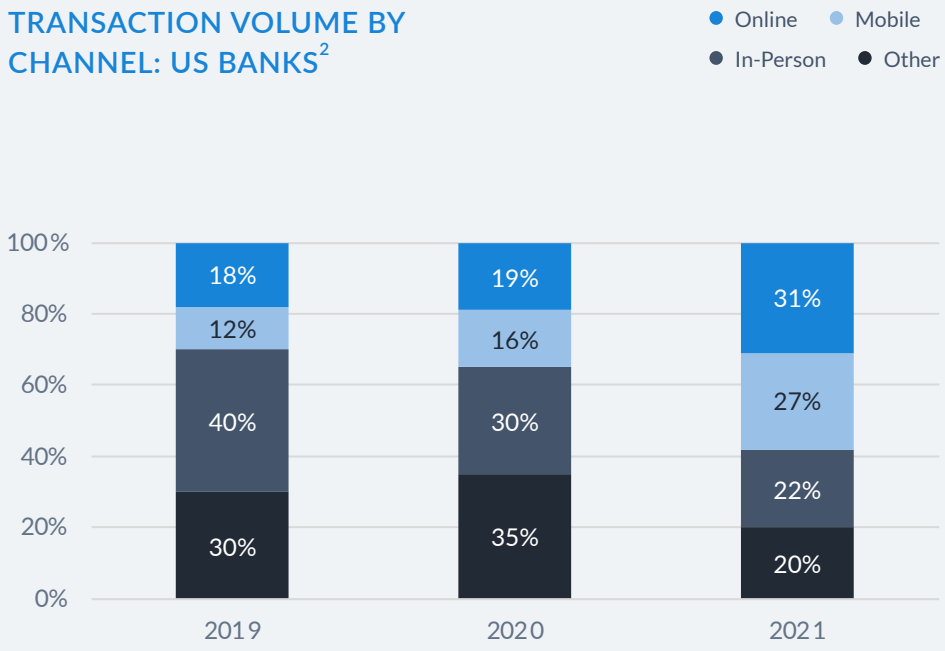
The Digital Banking BSA/AML/ OFAC & FRAUD Landscape

Shift to Online

Today, customers expect digital options from doctors, schools, jobs, and more. The same goes for banking.

- In recent years, in-person banking has rapidly declined while online and mobile transactions increased.
- Although use of digital banking applications had been increasing prior to 2020, the Covid-19 pandemic sped up the process.

TRANSACTION VOLUME BY CHANNEL: US BANKS[2]



In 2021, banking execs reported significant declines in in-person visits and increases in online and mobile transactions.

[2] LNRS, Jan 2022. "True Cost of Fraud 2021."

Challenger Bank Market Opportunity

A New Take on Banking

Although traditional banks were the first to experiment with digital banking, digital banks really began taking off in 2010 alongside an increase in mobile penetration.

- Digital banks (aka, digital banks, neobanks, or challenger banks) are fintech firms that offer apps, software, and other technologies to streamline mobile and online banking.
- Digital banks saw the opportunity to attract segments who are often overlooked by traditional banks, including younger generations, the underbanked, and customers with no credit.

They swapped dated branches, high fees, and limited hours for a digital approach. Their strategy is simple: Eliminate onboarding friction and attract as many customers as possible.

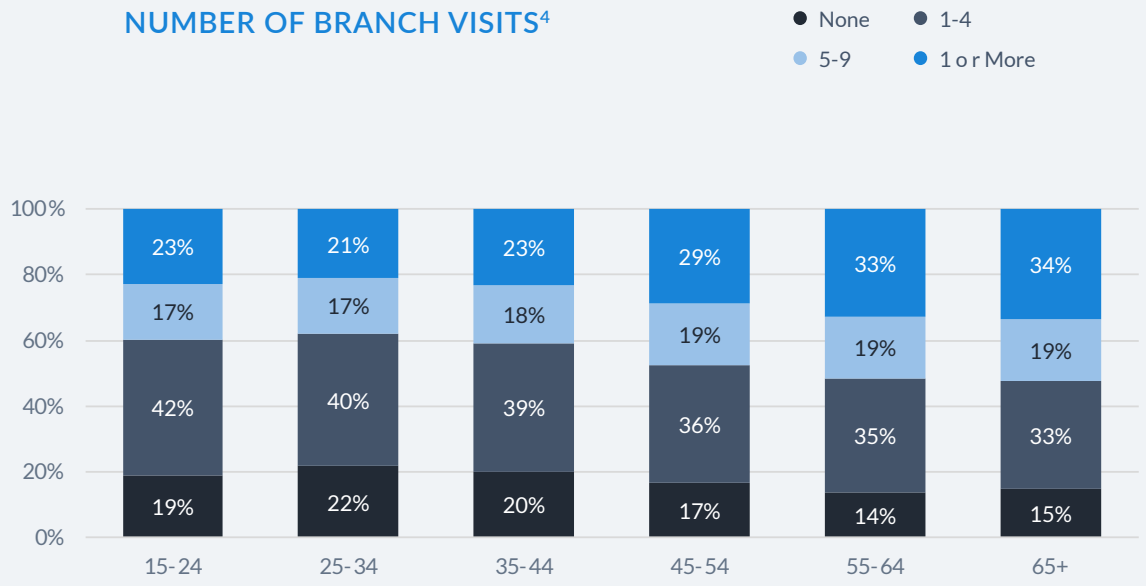
- Mobile-first design
- Lower fees
  - By employing instant approvals and being entirely digital, digital banks avoid costs associated with administrative employees and physical branches.
  - This makes it easier to offer lower fees than traditional banks.
- Digital access
  - The rise of digital banks came in part due to consumer behavior that shifted away from physical interactions.
- More inclusive
  - With lower fees and more accessibility, online options have made banking more inclusive, providing "millions of unbanked people with access to financial services."[3]

[3] https://www.finextra.com/blogposting/20863/how-digital-banking-services-are-encouraging-financial-inclusion

Appealing to Younger Generations

Although traditional banks have maintained a dominant role in financial services, digital banks are becoming the banks of choice for young people.

NUMBER OF BRANCH VISITS[4]



Younger generations are much less likely to visit bank branches.

Attracting younger demographics with years of future earnings growth is a big advantage for digital banks.

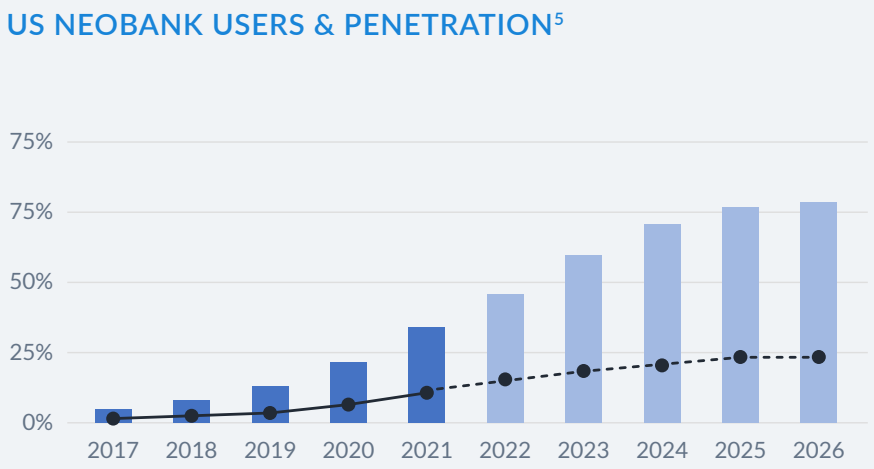
[4] FDIC, 2019. "How America Banks: Household Use of Banking & Financial Services. Number of visits within past year among banked households." www.fdic.gov/analysis/household-survey/index.html

Accelerated Growth

Digital banks began attracting a significant number of users in 2017 and are expected to continue with significant year over year growth through 2025.

Users & Penetration

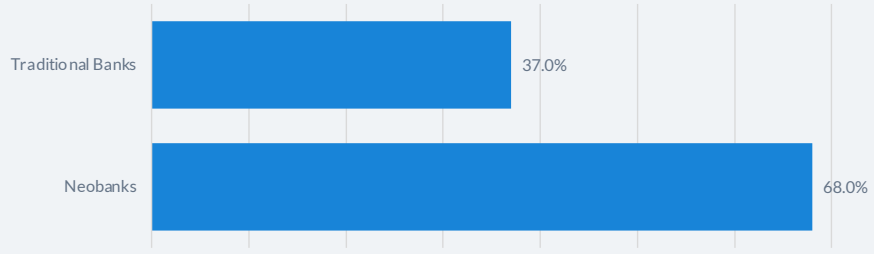
US NEOBANK USERS & PENETRATION[5]



Neobank customers and penetration increased by approximately 60% in 2021.

Transaction Growth

YEAR OVER YEAR TRANSACTION GROWTH 2021 VS 2020[6]



2021 was a banner year for digital banks in the U.S., with transaction volume growth significantly ahead of traditional banks.

[5] Statista, May 2021. "Digital Markets > Fintech > Neobanking." https://www.statista.com/outlook/dmo/fintech/neobanking/worldwide

[6] LNRS, Jan 2022. "True Cost of Fraud."

Rise in Fraud

Although digital transformation initiatives had been in motion in financial services for years, the pandemic forced banks to rush their online service developments.

- Along with stimulus payments provided by the U.S. government to offset the pandemic's impact on the economy, this hasty growth of online services ushered in a boom in fraud.
- As Javelin Strategy noted in their 2021 Identity Fraud Study, "The pandemic compelled companies to make quick adjustments to their business models, such as transitioning from in-person lending to online interactions with borrowers. Criminals pounced on new vulnerabilities presented by the explosion in remote loan originations and closings."

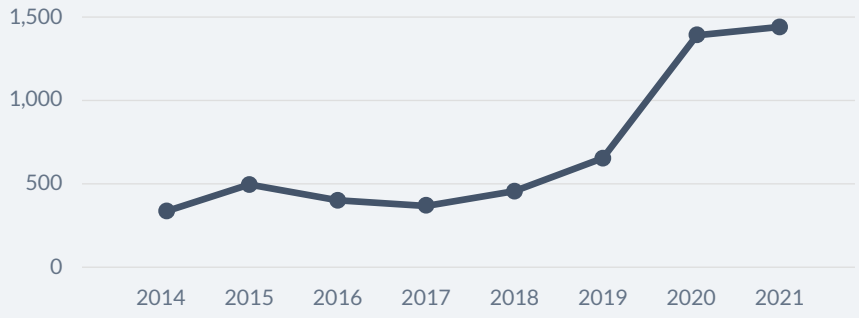
> The pandemic has created so many more points of vulnerability for families and businesses. Whether it's payment products meant to enhance convenience, remote operations, additional logins or even simply more time online, there is more opportunity now than ever for compromise."
>
> Paige Schaffer / CEO of Global Identity & Cyber Protection / GENERALI GLOBAL ASSISTANCE

Identity Theft

There has been a spike in identity theft reports in 2020.

- Volume continues to grow

IDENTITY THEFT REPORTS[7]

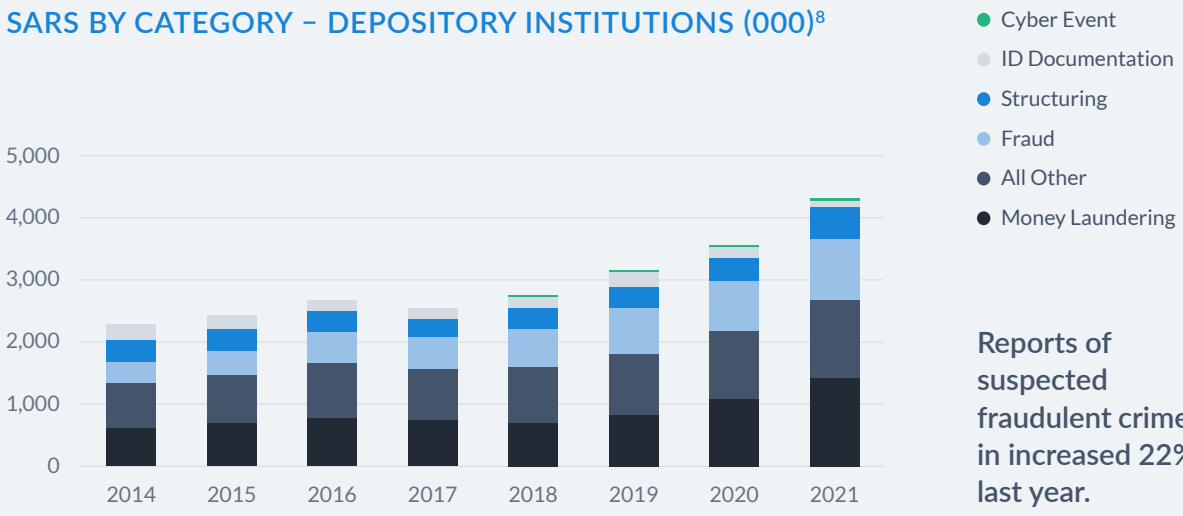


The number of reports from identity theft victims skyrocketed along with the pandemic.

[7] FTC, Mar 2022. "Consumer Sentinel Network Data Book 2021." https://www.ftc.gov/enforcement/consumer-sentinel-network/reports

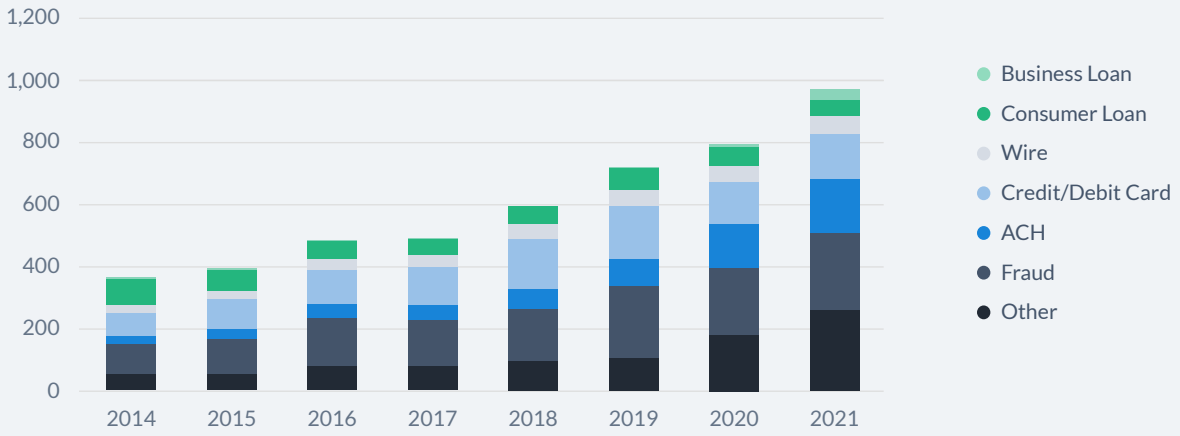
The number of Suspicious Activity Reports (SARs) submitted by banks to FinCEN, which include a large mix of crimes, showed gradual but steady increases since the pandemic.

SARS BY CATEGORY – DEPOSITORY INSTITUTIONS (000)[8]



Reports of suspected fraudulent crimes in increased 22% last year.

FRAUD SARS BY TYPE - DEPOSITORY INSTITIONS (000)[9]



Although it remains the smallest segment in the fraud category, business loan reports increased 184% over 2020 – possibly reflecting a rise in online merchant fraud.

[8]U.S. Treasury Financial Crimes Enforcement Network, 2014-2021. "Suspicious Activity Report Statistics. Depository institutions only." https://www.fincen.gov/reports/sar-stats/

[9]U.S. Treasury Financial Crimes Enforcement Network, 2014-2021. "Suspicious Activity Report Statistics. Depository institutions only." https://www.fincen.gov/reports/sar-stats/

The Biggest Fraud in a Generation

The speedy rollout of online banking applications and trillions distributed by government stimulus programs led to a perfect storm for fraud.

- The prevalence of Covid relief fraud has been known for some time, but the enormous scope and its disturbing implications are only now becoming clear.
- Even if the highest estimates are inflated, the total fraud in all Covid relief funds could rival the $579 billion in federal funds included in the 10-year infrastructure spending plan, according to prosecutors, government watchdogs, and private experts who are trying to account for the thefts.

The Biden administration imposed new verification rules in 2021 that administration officials say appear to have made a difference in curbing fraud. But they acknowledge that programs in 2020 sacrificed security for speed.

> The Small Business Administration basically said to people, 'Apply and sign and tell us that you're really entitled to the money.' And, of course, for fraudsters, that's an invitation.
>
> Michaek Horowitz / Chair, Pandemic Response Accountability Committee

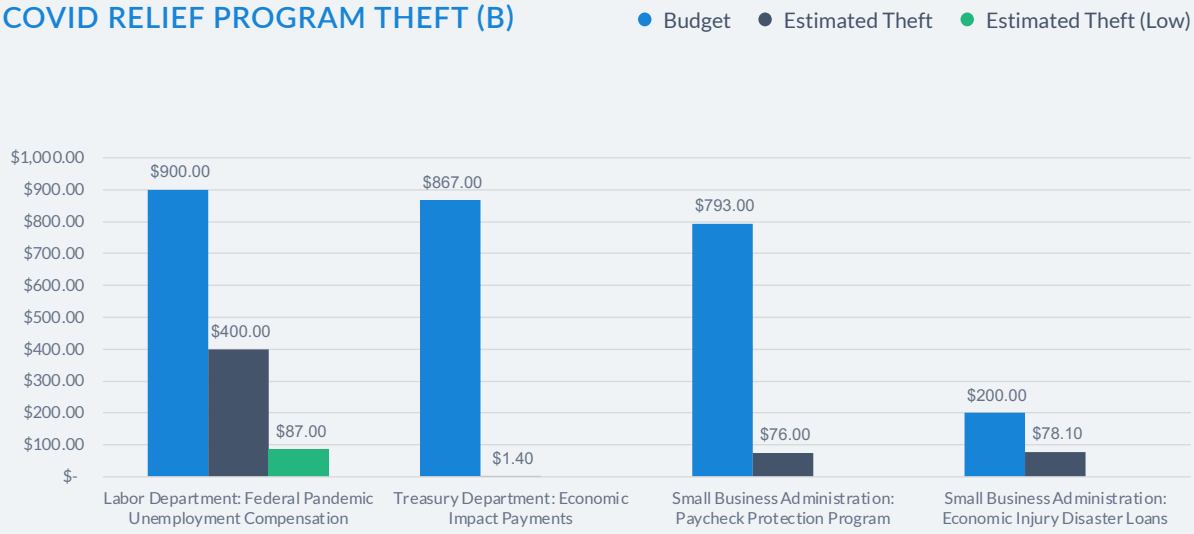
The criminal methodology varied depending on the program.

- Covid unemployment relief has been carried out by individuals or organized crime groups using stolen identities to claim jobless benefits from state workforce agencies disbursing federal funds.
  - Each identity is worth up to $30,000 in benefits.
- PPP theft worked differently – and was far more lucrative.
  - The program authorized banks and other financial institutions to make government-backed loans to businesses, loans that were to be forgiven if the companies spent the money on business expenses.
  - Experts say millions of borrowers inflated their numbers of employees or created companies out of whole cloth.

> Nothing like this has ever happened before. It's the biggest fraud in a generation.
>
> Matthew Schneider / Former U.S. Attorney, Department of Justice

To identify fraudulent theft, data scientists with the Pandemic Response Accountability Committee are using AI to analyze 150 million records for fraud patterns.

COVID RELIEF PROGRAM THEFT (B)



At least half of the theft from the Unemployment Compensation fund occurred by criminals overseas.[10]

Note: Indicates money stolen from government programs. Does not include fraud related to relief programs perpetrated against individuals.

[10]NBC News, Mar 28, 2022. "Biggest Fraud in a Generation: The Looting of the Covid Relief Program Known as PPP." https://www.nbcnews.com/politics/justice-department/biggest-fraud-generation-looting-covid-relief-program-known-ppp-n1279664

Challenger Bank Regulatory & Compliance Issues

While the rise in fraud explains some of their compliance-related problems, digital banks appear to have broader issues with adherence.

- Many of these companies have focused hiring on tech-savvy developers and marketers who often do not have a banking background.
- Like many fintechs, they are hyper-focused on growth, and tend to hire compliance officers relatively late in their development.[11]

The Digital Bank & Traditional Bank Ecosystem

Unlike some disruptive business models that replace the incumbents, digital banks and traditional banks have formed an ecosystem. Traditional banks often serve as the back-end for deposit and loan services while digital banks provide new business via consumer-friendly mobile applications. In fact, most digital banks can focus on the customer experience only because they've partnered with a large bank that navigates an incredible amount of regulation, such as a banking license in each state.

> A lot of people set out saying, 'We are going to displace the banks.' We realized along the way that you really have no choice but to work with the banks."
>
> Sheel Mohnot / Co-Founder, Better Tomorrow Ventures

The "Rent a Charter" Model

For example, digital banks that aren't licensed to underwrit e loans can offer this service by passing the loan request to a traditional bank, which originates the loan and immediately sells it to the digital bank. In this case, digital banks are relying on the "valid when made" principle, which allows loans that meet the relevant legal requirements at inception to be transferred to other entities.

[11]Finty, May 7, 2021. "Ten Fintechs That Failed (and Why)." https://finty.com/us/research/fintech-failures/

This "rent a charter" model has led some to accuse digital banks of peddling regulatory arbitrage, creating financial risks, and undermining the regulations designed to strengthen the financial system's stability.[12] This criticism has prompted some digital banks to clearly state "we are not a bank" on their materials and provide clarity about the services their traditional bank partner provides.

Banks that do have charters would of course be subject to the full panoply of Bank Secrecy Act, USA PATRIOT Act and AML regulations. Even the non-chartered would need controls in these areas to stay ahead of criminals and fraudsters.

Increased Attention From Regulators

This clarity may not protect them from regulatory scrutiny however. Traditionally, only banks and credit unions have been subject to federal supervision, but Congress gave the CFPB broader authority when it was created in the wake of the 2008 finanical crisis. In April, the CFBP invoked its authority to examine "nonbank" financial companies – which includes many digital banks – in order to "protect consumers and level the playing field between banks and nonbanks."[13]

Robinhood represented a lack of regulatory understanding when it advertised checking and savings accounts with a 3% yield in 2019. Regulators noted the money wouldn't be insured by either the Federal Deposit Insurance Corporation or the Securities Investor Protection Corporation and referred the matter to the Securities and Exchange Commission.[14] Needless to say, Robinhood canceled the product launch.

For the most part however, regulators have taken a relatively light approach to digital bank supervison. Some have expressed optimism for the segment's potential to serve underbanked communities.[15] For now, traditional banks remain responsible for the bulk of the industry's fraud and anti-money laundering compliance requirements, but this is likely to change as digital banks account for a greater share of consumer banking services.

> Given the rapid growth of consumer offerings by nonbanks, the CFPB is now utilizing a dormant authority to hold nonbanks to the same standards that banks are held to."
>
> **Rohit Chopra / Director, Consumer Financial Protection Bureau**

[12]Duke University School of Law, Global Financial Markets Center, Jan 23, 2020. "The Rise of Rent-a-Charter: Examining New Risks Behind Bank-Fintech Partnerships." https://sites.law.duke.edu/thefinregblog/2020/01/23/the-rise-of-rent-a-charter-examining-new-risks-behind-bank-fintech-partnerships/

[13]Consumer Finance Protection Bureau, April 25, 2022. "CFPB Invokes Dormant Authority to Examine Nonbank Companies Posing Risks to Consumers." https://www.consumerfinance.gov/about-us/newsroom/cfpb-invokes-dormant-authority-to-examine-nonbank-companies-posing-risks-to-consumers/

[14]San Francisco Chronicle, Nov 27, 2019. "Robinhood Drops Plans to Start a Bank; Brokerage Clients Still Waiting for Interest on Cash." https://www.sfchronicle.com/business/networth/article/Robinhood-drops-plan-to-start-a-bank-brokerage-14867571.php

[15]Georgetown University Law Center, 2 Dec. 2016. "Remarks By Thomas J. Curry Comptroller of the Currency Regarding Special Purpose National Bank Charters for Fintech Companies." www.occ.treas.gov/news-issuances/speeches/2016/pub-speech-2016-152.pdf.

Neobanks: Ideal Targets for Money Laundering & Fraud

Why Are Digital Banks Susceptible to Money Laundering & Fraud?

> There's no risk of needing to show identification in person, no surveillance video to show who's utilizing the bank account. Transferring and receiving funds to and from co-conspirators is pretty easy."
>
> Kyle Kinney / Detective, Delray Beach, FL Police Department

Unfortunately, by reducing friction and opening the door open to so many customers, digital banks have inadvertently made themselves the perfect target for criminals.

- Cybercriminals target digital banks, expecting lower security hurdles than they'd find at a larger institution.
- There's no in-person document review, and fraudsters outside of the U.S. can easily submit new customer or loan applications.
- With fraudsters becoming more sophisticated, they can easily manipulate documents to bypass KYC checks during customer on-boarding.
- Many digital banks such as Chime, Current, and Varo Bank, do not require "hard" credit checks to open an account – making them even more at risk for fraud compared to traditional banks.[16]

[16]Forbes, June 14, 2021. "What Is a Neobank?" https://www.forbes.com/advisor/banking/what-is-a-neobank/

> The biggest underestimated issue in digital banking is the potential for fraud. Since we began our efforts to deliver a digital solution, we've put fraud and risk management at the forefront of everything."
>
> Michael Butler / CEO, Grasshopper Bank

Traditional banks that partner with digital banks also open the possibility of an exponential rise in fraud or cyberattacks through these partners and their technology providers.

As cryptocurrencies are largely unregulated, digital banks and fintechs that manage these digital assets have become a prime target for hackers as well.[17]

Insufficient Risk Management, AML & OFAC Controls

Another likely reason for large volumes of fraud at digital banks is new risk management processes and less experienced AML, anti-fraud, and OFAC compliance teams. Staff at many digital banks tend to have more experience in technology than banking, which leads to consumer-friendly applications, but less developed AML, fraud investigations and OFAC compliance.

In a summary of their findings on customer due diligence practices at six unnamed digital banks, the UK's Financial Crimes Authority (FCA) noted "more needs to be done by the challenger banks sector as a whole in light of the areas of improvement we identified. The weaknesses we found create an environment for more significant risks of financial crime to occur both when customers are onboarded and throughout the customer journey."[18]

Risk management deficiencies identified by the FCA include:

- Insufficient customer information collected at account opening, "resulting in an incomplete assessment of the purpose and intended nature of a customer's relationship with the bank."
- Customer risk assessments that were undeveloped, lacking in detail or in some cases, nonexistent.
- Identifying and monitoring high risk customers (CDD/EDD).

[17]ResearchGate, July 2020. "Disruptions and Digital Banking Trends." https://www.researchgate.net/profile/Luigi-Wewege/publication/343050625_Disruptions_and_Digital_Banking_Trends/links/5f136f93a6fdcc3ed7153217/Disruptions-and-Digital-Banking-Trends.pdf

[18]Financial Conduct Authority, April 2022. "Financial Crimes Controls at Challenger Banks." https://www.fca.org.uk/publications/multi-firm-reviews/financial-crime-controls-at-challenger-banks

- Inadequate oversight of financial crime programs.
- Controls that failed to keep up with changes to the company's business model.
- Ineffective management of transaction monitoring alerts.
- Concerns with Suspicious Activity Reports.
- Inconsistent processes and in some cases, lack of formal risk management procedures. The report notes one digital bank which lacked an enhanced due diligence process, meaning "it did not have the capability to identify customers that may present a high or higher risk of money laundering or terrorist financing and therefore couldn't mitigate those higher risks effectively."

Underscoring the need for thorough identity verification at the account opening stage, the FCA noted some of the banks instituted programs to address the concerns raised, which "may result in them potentially rejecting a larger number of new customers at onboarding."

> In addition, where these challenger banks promote the ability to open accounts very quickly to attract customers, there is a risk that information gathered at the account opening stage is insufficient to identify higher risk customers."
>
> Financial Conduct Authority / From the April 2022 FCA Report, "Financial Crimes Controls at Challenger Banks."[19]

OFAC compliance applies to every "U.S. person" including all U.S. citizens wherever located, and all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Enforcement action for violations of OFAC sanctions programs are "zero tolerance," and include the use of digital currencies or other emerging payment systems to conduct proscribed financial transactions and evade U.S. sanctions. In October 2021, OFAC published a guide for OFAC compliance in the virtual currency industry, and guidance on potential sanctions risks for facilitating ransomware payments. This type of activity is within the concerns facing challenger banks when setting up necessary interdiction mechanisms for OFAC compliance.

[19]Financial Conduct Authority, April 2022. Financial Crimes Controls at Challenger Banks. https://www.fca.org.uk/publications/multi-firm-reviews/financial-crime-controls-at-challenger-banks

Who Targets Digital Banks?

From Crime Rings to Rogue Nations

Individuals and small fraud rings continue to snatch credit card applications from mailboxes, but the bulk of today's fraudsters are well-resourced, global criminal organizations.

- Criminal organizations apply stolen proceeds to a range of crimes, including human trafficking and narcotics production.
- One criminal initiative, later known as FASTCash, provided yakuza associates in Japan with fraudulent credit cards to withdraw cash from ATMs. The low-level criminals involved were unaware that the ringleader was based in China and funneled the proceeds to the North Korean government.[20]

Leveraging Sophisticated Technology

Crime rings employ sophisticated technology to circumvent bank defenses and scale their operations.

- AI is used to "learn patterns of normal user behavior inside a network"[21] to bypass security systems.
- Machine learning is applied to approved and denied loan applications, which trains the system to create applications that are increasingly difficult to detect.
- This allows fraudsters to evade traditional legacy systems, which start with a "top down" picture of what a fraudulent application looks like. These systems focus on static rules like multiple addresses, or a high volume of credit inquiries.

The U.S. government is taking the threat seriously, with the U.S. Financial Crimes Enforcement Network including transnational criminal organization activity, cybercrime, and fraud in their *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*.[22]

[20]The New Yorker, April 26, 2021. "The Incredible Rise of North Korea's Hacking Army." https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army

[21]The Wall Street Journal, November 15th, 2017 "Era of AI-Powered Cyberattacks Has Started." https://www.wsj.com/articles/artificial-intelligence-transforms-hacker-arsenal-1510763929

[22]FinCEN, June 30, 2021, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities." https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

Types of Fraud Facing Digital Banks

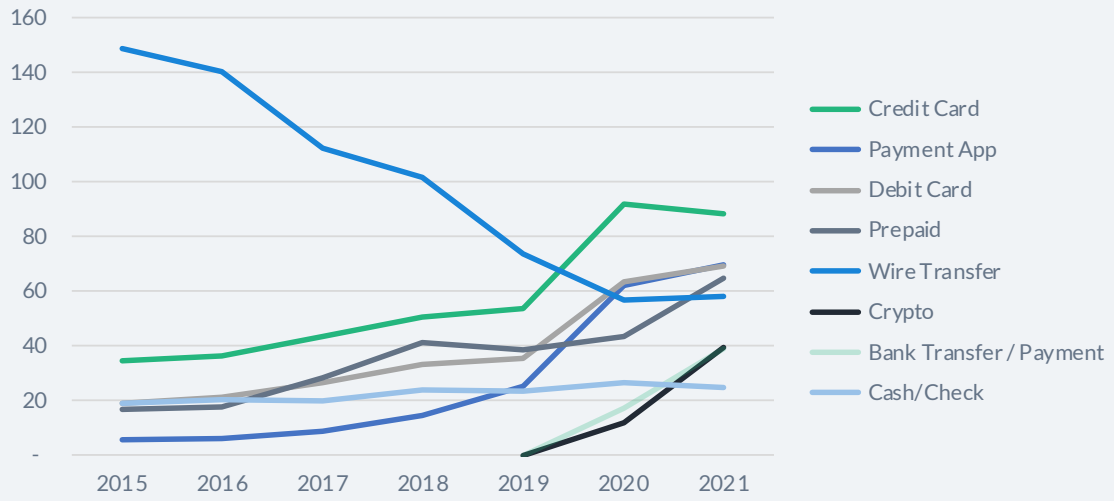
Fraud is an issue for every financial institution, but what types of fraud are digital banks particularly susceptible to?

P2P Fraud

After credit cards, payment apps were related to the majority of fraud cases reported by consumers and law enforcement.

> Digital-focused banks have a target on their backs because fraudsters know that the banks want to make the user signup flow and banking experience as seamless as possible."
>
> **Kevin Lee / VP of Trust & Safety, Sift**

FRAUD REPORTS BY PAYMENT METHOD (000)[23]



Fraud cases involving cryptocurrencies had the biggest increase, up 236% from 2020.

Account Takeover

As Forbes noted in December, "Account takeovers are another scam that fintechs like Chime are particularly susceptible to, because fraud rings often target new technology, thinking it's more likely to have holes."[24]

Account takeovers occur when a criminal obtains access to an online account, often by hacking the user's password. While account takeovers happen to traditional banks as well, fraudsters appear to be focusing their efforts on digital banks.

[23]FTC, 2015-2021. "Consumer Sentinel Network Data Book." https://www.ftc.gov/enforcement/consumer-sentinel-network/reports

[24]Forbes, Dec 3, 2021. "Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards." https://www.forbes.com/sites/elizahaverstock/2021/12/03/fintechs-fraud-problem-why-some-merchants-are-shunning-digital-bank-cards/?sh=190377875bd5

ACH Fraud

ACH, the system behind most bank-to-bank transfers in the U.S., was developed in the 1970s and still lacks real-time verification. When a customer requests an ACH transfer, the receiving bank typically makes the money available immediately, although it can take days for the transaction to settle. As the diagram below shows, fraudsters can use that time to their advantage.

Authorized Push Payment Fraud

Also known as the "me-to-me scam," no other form of fraud causes more conflict between victims and their banks. While financial institutions are generally quick (and often required) to reimburse customers for fraudulent losses, this scam falls in a legally gray area that banks often refuse to accept responsibility for.

Unlike fraud that consumers are unaware of until they see a charge or withdrawal, authorized push payment fraud occurs when a scammer convinces their victim to provide sensitive information or transfer funds. While the mechanics vary, it typically involves a scammer reaching out directly to a consumer, posing as a bank or payments service representative to gain their trust.

Banks argue that they're only responsible for "unauthorized" transactions, which isn't applicable when the victim initiates the transfer. In guidance issued in 2021, the CFPB stated that banks are responsible for losses that are "initiated by a person other than the consumer without actual authority to initiate the transfer," including those who obtain a victim's device through fraud or robbery. This guidance, however, still fails to clarify whether banks are responsible for fraudulently induced transfers when the victim presses the "send money" button.

The CFPB has been flooded with complaints about this type of fraud and is considering how to address it.

Chargeback Fraud

Also known as friendly fraud, it occurs when a customer requests a refund, by disputing charges through their bank. Customers will claim that an order did not arrive, a product was broken, or that they did not purchase an item in the first place.[25]

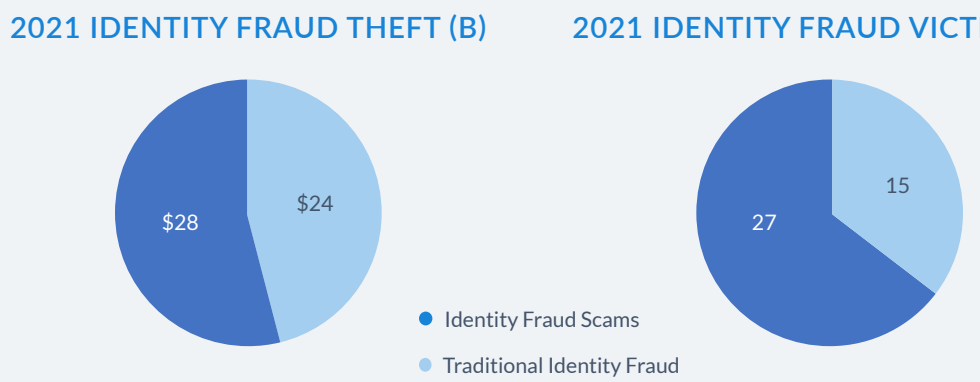
[25]Cardinal Commerce, "What is Chargeback Fraud." https://www.cardinalcommerce.com/fraud/chargebacks/what-is-chargeback-fraud

Identity Fraud

In their research, Forbes also found that fintech providers also appear more likely to be susceptible to identity fraud.[26]

Identity fraud (commonly referred to as identity theft) is the use of an individual's personal information to achieve illicit financial gain.

- Identity fraud *scams* are a subset where criminals directly influence a consumer to divulge personal information or conduct a transaction.



Identity fraud scams (where fraudsters solicit personal identifiable information [PII] directly from the victim) now outnumber traditional identity fraud (where PII is stolen secretly).[27]

Identity fraud is a growing problem that has expanded in new ways since the onset of the COVID-19 pandemic, which prompted wide changes in digital behaviors.

Aside from the money stolen, identity fraud wreaks havoc with a digital bank's customer relationships. Nearly one-third of identity fraud victims say their financial services providers did not satisfactorily resolve their problems, and 38% of victims closed their accounts because of lack of resolution at the financial institution where their fraud occurred.[28]

[26]Forbes, Dec 3, 2021. "Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards." https://www.forbes.com/sites/elizahaverstock/2021/12/03/fintechs-fraud-problem-why-some-merchants-are-shunning-digital-bank-cards/?sh=190377875bd5

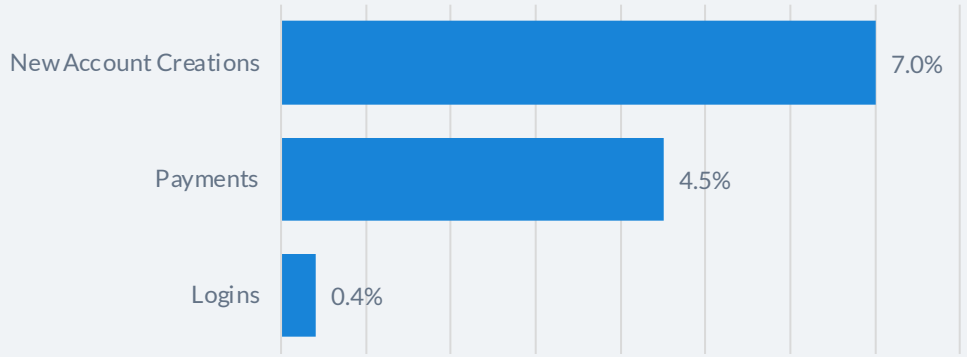
[27]Javelin Strategy, Mar 2021. The 2021 Identity Fraud Study. https://www.javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020

[28]Javelin Strategy, Mar 2021. "The 2021 Identity Fraud Study." https://www.javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020

New Account Fraud

At this early stage in their development, the majority of neobank revenue stems from new account openings, which are especially attractive to fraudsters.

FINANCIAL SERVICES: ATTACK RATE BY TRANSACTION TYPE[29]



New account creations have the highest attack rate across transaction types.

Identity theft related to bank fraud has overwhelmingly focused on new accounts since the start of the pandemic.

Synthetic Identity Fraud

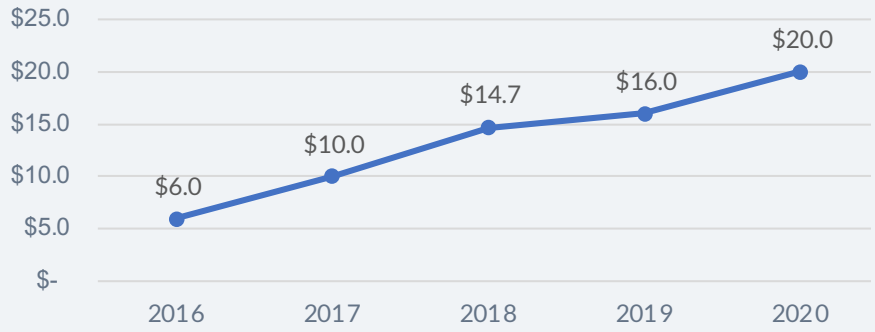
As defined by the Federal Reserve, synthetic identity fraud "is the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain."

Criminals create synthetic identities using PII stolen or purchased on the dark web, open bank accounts, and nurture these accounts over time, making prompt credit card or loan payments. Once they've built up their credit score and worthiness, they'll "bust out," walking away with a substantial theft.

Annual losses due to SIF have increased dramatically, with FiVerity estimating theft reached $20 billion in 2020.

[29]LNRS, Mar 2022. "LNRS Cybercrime Report: Jul – Dec 2021."

ANNUAL SIF LOSSES[30]



FiVerity estimates synthetic identity fraud is responsible for $20B in losses.

This growth is in part due to consistent data breaches targeting businesses and consumers. Criminals invested heavily in stealing PII between 2016 to 2018 and have focused on monetizing this information since. In addition to stealing from banks via identity fraud, criminals use consumer information like login credentials to defraud companies in a range of industries.

PERSONAL IDENTITY STOLEN (M)[31]

Although thefts of PII have been in decline, fraudsters have plenty to work with: 1.5 billion identities have been stolen in the past three years alone.

[30]FiVerity, Oct 2021. 2021 Synthetic Identity Fraud Report.

[31]ITRC, Jan 2022. "2021 in Review: Data Breach Annual Report." https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

Jobless Claims

Another scheme digital banks are particularly at risk for is jobless claims. Individuals will apply for unemployment benefits in states they do not live in. They then set up direct deposit into a digital bank checking account like Chime, Cash App, or Green Dot.

Broader Money Laundering and Human Trafficking/Smuggling Concerns

The broader money laundering concerns affecting challenger banks is not much different than traditional banks, just that the speed of the transaction, relative remoteness (no branches where bank employees can see you and recognize you over time) and the digital nature of all payments are attractive to criminals. The above discussed fraud concerns are all avenues that can be used to launder illicit funds, in addition to the direct fraud implications for customers and victims of myriad fraud and scams. There is nuance involved as money laundering can and does encompass the fraud avenues, but sometimes fraud is just "fraud," like a romance scam.

Digital banks typically have leaner staffing, quicker transaction processing and streamlined know your customer (KYC) and customer due diligence (CDD) processes and controls, making them attractive to criminals.

There are two large and related concerns:

Money Mules

Illicit funds originating from criminal online activity, human trafficking, and drug trafficking is electronically transferred through accounts set up by the recruited mules. This is the "layering" step of money laundering – separating and adding layers between the crimes and the victims to throw off law enforcement. Virtual currency, wires, and ACH are ways challenger banks would be used in the scheme. All the funds appear to be legitimate when the individual initially opens the account and begins receiving incoming transfers. The mule is then instructed to send the funds abroad or to other banks. Cryptocurrency transactions, with added anonymity and a key component of these new banks, is yet another layer and even harder to trace. Transactions are typically small but numerous ("smurfing") to try and avoid detection software and scenarios relying on transaction values.

Access to internet and computers is "easy" compared to lugging in cash and buying money orders and bank checks or depositing and wiring out. The absence of the cash component makes things easier. Stolen identities, opening accounts in a virtual environment, and false documents are all the beginning stages of the process, and challenger banks are front-and-center due to their remote structure.

Jobless Claims

Another scheme digital banks are particularly at risk for is jobless claims. Individuals will apply for unemployment benefits in states they do not live in. They then set up direct deposit into a digital bank checking account like Chime, Cash App, or Green Dot.

Smurfing

Smurfing involves moving large amounts of illicit money by a series of small "under the radar" transactions. Challenger banks process large volumes of ACH and wires so the risk is heightened. Smurfing typically ties into money mule operations. In the past, cash was deposited in small amounts and then moved out via Bank checks or wires. In the 21st century, "crypto smurfing" has taken over the game.

Challenger banks would most likely function as a middleman in some fashion, especially if cash needs to be deposited at a traditional bank, then moved digitally to purchase and transact. Now the funds are digital and can move around the world instantaneously.

Key Pillars of KYC (Know Your Customer) and AML (Anti Money Laundering)

Know Your Customer procedures are a critical function to assess customer risk. Effective KYC involves knowing a customer's identity, their financial activities, and the risk they pose (e.g., fraud or illegal funds and transactions).

New technological developments continue to drive KYC solutions forward. From biometric data to AI, technology is offering better ways to identify customers, run due diligence checks, and perform ongoing monitoring.

When gathering KYC information to assess customer risk, identify the following areas:

- Assess what you need and establish customer identity
- Explore to find the answers
- Organize to make meaningful and understand the nature of the customer's activities
- Present to inform and defend – assess AML risks associated with the customer for purposes of monitoring the customer's activities

Impact of Money Laundering & Fraud

Digital fraud's impact on digital banks extends far beyond financial losses.

Platforms Declined

Due to overwhelming volumes of fraud, some massive companies stopped accepting credit cards issued by digital banks. Rental car agencies like Enterprise, Avis, and Hertz stopped accepting digital bank cards as a form of payment when picking up a car, and some hotel franchises adopted similar policies.

Robinhood has banned LendingClub and Green Dot, with a spokesperson explaining that "Robinhood prevents transfers from routing numbers that display a high pattern of return and fraud rates." Robinhood has banned Metropolitan Commercial Bank and other lending partners due to high rates of fraud as well.[32]

In another example, a payment processing company that works with hundreds of merchants blocked transactions from a prominent digital bank last year due to a massive volume of ACH fraud.[33]

Customer Service Suffers

In addition to a lack of physical branches, digital banks save money by hiring fewer administrative employees. Although automated processes and online interfaces provide efficiencies, they can be a painful barrier to customers who are desperately trying to resolve a fraud-related emergency.

In their attempt to counter fraud, digital banks have also faced backlash for closing a high volume of legitimate customer accounts. One customer discovered he was locked out of his account, which had over $10,000 in deposits, when his card was declined at Applebee's. After reaching out to his digital bank he received an email informing him that they "made the decision to end our relationship with you at this time and your spending account has been closed".[34]

This is likely why digital banks such as Chime have generated a high rate of complaints, with 920 filed at the Consumer Financial Protection Bureau since April 15, 2020. For context, Wells Fargo, which has a spotty reputation and six times as many customers, had 317 CFPB complaints in the same period.[35]

[32]Forbes, Dec 20, 2021. "With Fraud Growing, Robinhood Becomes Latest Fintech to Block Customers from Transferring Money from Certain Banks." https://www.forbes.com/sites/jeffkauflin/2021/12/20/with-fraud-growing-robinhood-becomes-latest-fintech-to-block-customers-from-transferring-money-from-certain-banks

[33]Forbes, Dec 3, 2021. "Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards." https://www.forbes.com/sites/elizahaverstock/2021/12/03/fintechs-fraud-problem-why-some-merchants-are-shunning-digital-bank-cards/?sh=190377875bd5

[34]ProPublica, July 6th, 2021, "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money" https://www.propublica.org/article/chime

[35]ProPublica, July 6th, 2021, "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money" https://www.propublica.org/article/chime

Government Penalties

Although digital banks have largely avoided the attention of regulators, this situation appears to be changing as they become a larger force in financial services. Like traditional banks, digital banks with inadequate fraud and anti-money laundering programs are subject to financial penalties and in a worst-case scenario, complete shutdown.

Although it wasn't fraud related, LendUp's series of compliance fails saw it shut down by the CFPB in January 2022. The agency found that previous fines had failed to stop the company's deceptive lending practices and revoked the digital bank's ability to offer loans (in good news for its customers, the company forgave all outstanding loans).

This action, along with the CFPB's announcement that it was invoking its right to monitor non-bank fintechs, sent a clear signal about its aggressive stance. Although some lawmakers are questioning whether the agency is over-stepping, digital banks and a range of fintechs should expect increased scrutiny.

In Europe, German neobank N26 was fined €4.25 million for weak anti-money laundering practices [36] and UK's Monzo was investigated for insufficient anti-money laundering and financial crime controls.[37]

In 2019, a whistleblower highlighted compliance concerns at Revolut, prompting an inquiry from the UK's Financial Conduct Authority. The whistleblower expressed concerns that transactions for sanctioned individuals with ties to chemical weapons and terrorism were moving forward after the company turned off relevant internal controls.[38]

> The fintechs that come into this space get their venture funding, and they don't always invest in compliance and regulations because those efforts are not part of the growth trajectory or part of the product design."
>
> Laurel Loomis Rimon / Former Deputy Chief, U.S. Department of Justice

As FinCEN cracks down on transnational criminal organizations and the fraud that funds them, digital banks will have to focus additional resources on fraud prevention.[39]

[36]Computer Weekly.com, September 30th, 2021, "Digital bank fines by regulator due to weak anti-money laundering controls." https://www.computerweekly.com/news/252507492/Digital-bank-fined-by-regulator-due-to-weak-anti-money-laundering-controls#:~:text=German%20neo%20bank%20N26%20has,reports%20in%202019%20and%202020

[37]BBC, July 31st, 2021 "Monzo bank in money laundering rules investigation." https://www.bbc.com/news/business-58033700

[38]BBC News, April 2, 2019 "Revolut whistleblower had concerns over CEO conduct and compliance." https://www.bbc.com/news/technology-47751945

[39]PYMNTS.com, July 9th, 2021, "digital banks, Small FIs Face Heavy Lift Building Compliant AML Systems From Scratch" https://www.pymnts.com/aml/2021/digital banks-small-financial-institutions-face-heavy-lift-building-compliant-systems/

OFAC Action

On April 21, 2022, the Office of the Comptroller of the Currency (OCC) entered into a consent order with Anchorage Digital Bank, National Association (Anchorage), for its violations of the Bank Secrecy Act (BSA)/anti-money laundering (AML) program, internal controls for customer due diligence, and procedures for monitoring suspicious activity, BSA officers and staff, and training. This is the first penalty of this type handed down to a "digital" bank.

On May 6, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Blender.io (Blender), which is used by the Democratic People's Republic of Korea (DPRK) to support its malicious cyber activities and money-laundering of stolen virtual currency. This was the first ever sanction of this type of activity. While not directly related to challenger banks, the move is relevant as an indication that OFAC is "regulating by enforcement" in its fight against criminals abusing digital currency and emerging payments systems.

Strained Relationship with Lending Partners

As noted earlier, many digital banks rely on traditional financial institutions in order to offer consumer loans. Notable digital bank lending partners include Community Federal Savings Bank, Coastal Community Bank, and WebBank.

As instances of fraud increase, these lenders can also be blocked by merchants and payment processors. The threat of being blocked or simply being a gateway for fraudsters into the payments system will make these banks hesitant to work with digital banks moving forward.

Fighting Back

Criminals are constantly evolving and becoming more sophisticated. However, fraud solutions also continue to innovate to keep up with these new threats. Solutions using machine learning, artificial intelligence, and encryption make interbank collaboration, document review, and identity verification easier while generating fewer false positives.

Machine Learning

As we touched upon earlier, fraudsters are harnessing the power of automation and machine learning to bypass legacy BSA/AML and fraud detection systems.

However, banks can use the same technology to identify these attacks. Instead of assuming what a fraudulent account, suspicious activity, or money laundering looks like, machine learning takes a "bottom up" approach. This involves searching profiles for patterns that match those of recently confirmed fraudsters and money laundering schemes, along with patterns and behaviors indicative of human trafficking and smuggling. Instead of checking against a set of static rules. This allows systems to adapt as criminals' tactics evolve.

Further, machine learning allows institutions to continue their rapid growth, but more importantly to grow safely with minimal friction.

Collaborative Approach

Recent studies indicate that the average bank has 9-12 anti-fraud solutions.[40] While these disparate tools are obviously meant to mitigate fraud's threat, the volume of data generated can easily overwhelm fraud investigators.

The financial industry was estimated to spend 10.7 billion on IT AML-KYC compliance and operations to reach a total of 26.4 billion globally in 2021.

Automated software (artificial intelligence and machine learning) are key components in compliance regimes in the 21st century.

By employing a collaborative approach to AML and fraud detection and prevention, digital banks can keep up with sophisticated criminals and get the most out of their AML and anti-fraud investment. Instead of rip and replace, collaborative systems integrate with a financial institution's current set of AML detection scenarios and fraud-fighting tools. The consolidated data from each tool informs recommendations, and the collaborative system provides transparency into the effectiveness of each component.

As global criminals adopt AI, automation, and other cyber approaches to their money laundering and fraud schemes, collaborative systems also integrate with cybersecurity department tools and data sets. Instead of data overload, AML, anti-fraud, and cybersec teams have a single, comprehensive view of the threats facing their organization.

Collaborative models collect data from multiple banks to identify patterns of fraudulent activity with a higher degree of accuracy. They provide a volume of data and computing power that simply isn't available with a model that's limited to a single bank's data set.

In addition to the volume of data required for machine learning, this solution provides advantages for model governance. While internal models developed by a bank become dated shortly after they're implemented, outsourcing to third party experts ensures the model is constantly adjusted to reflect changes in the marketplace. Working with encrypted data that obscures PII also limits the likelihood that the model developers will inadvertently insert their biases into the algorithms.

These models are necessarily hosted in the cloud, which is concerning to banks that mandate on-premises solutions in order to protect sensitive customer data. The security offered by confidential computing however, is allowing banks with the most stringent data protection policies to access the benefits of cloud-based models.

Confidential Computing

Confidential computing is an emerging industry initiative focused on a particularly thorny problem – securing data in use. The goal of this effort is to enable encrypted data to be processed in memory while lowering the risk of exposing it to the rest of the system, thereby reducing the potential for sensitive data to be exposed while providing a higher degree of control and transparency for users.

[40]Lexis Nexis Risk Solutions, 2021, "True Cost of Fraud™ Study", https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#financialservices

As information is especially vulnerable when it's being delivered, this point of failure is where most encryption standards are focused. In addition to protecting data in transit (moving over a network connection) and at rest (in storage and databases), Confidential computing eliminates the remaining data security vulnerability by protecting data in use — during processing or runtime.

Unlike the many encryption protocols focused on protecting data when it's being sent, confidential computing protects data whether it's in transit, at rest, or in use. It also provides a new level of control over the data shared and its accessibility, making more banks comfortable with the idea of alerting a network of financial institutions and law enforcement agencies to identified fraudsters.

BSA/AML/OFAC & Fraud Risk Assessment

Money laundering and fraud awareness, along with OFAC sanctions and compliance. must be promoted within neobank organizations to help all bank employees understand the risk in these areas and its potential impact.

From a governance perspective, management should be aware of risks identified as part of the risk assessment process, including both internal and external risk factors. These factors drive the greater promotion of money laundering, fraud, and OFAC sanctions awareness throughout the organization. The risk assessment process will ultimately identify the key areas that will require specific AML, anti-fraud, and OFAC internal controls and enhance the overall control environment of the organization, reducing the likelihood and impact of losses due to money laundering, fraud, and OFAC violations.

The business model of a digital bank requires additional efforts during this process to address the unique risks that these institutions face. The risk assessment process should be collaborative in nature, and be supported by the board of directors, the audit committee, and senior management. Generally, the BSA/AML/OFAC and fraud risk assessments will cover areas including but not limited to products and services, customer base, geography, financial reporting, asset misappropriation, regulatory compliance, and legal and external due diligence (including third parties such as vendors, customers, etc.). Integrating the risk assessment process within all levels of the organization helps promote fraud awareness to bank employees, as well as to third parties of the organization.

As previously discussed in this article, a large portion of risk of loss and exposure to money laundering for neobank organizations is within the external fraud category, specifically fraud committed by customers, with a smaller portion to pure money laundering via money mules and "smurfing." While appropriate controls within the organization should be in place to prevent and detect internal fraud, the tech-based nature of digital banks presents significant opportunity for customers to commit fraud and use this avenue to launder money and finance further illicit activity, including terrorist financing.

Ultimately, digital banks are far more susceptible to fraud risks such as synthetic identity fraud, account takeover, and other forms of advanced fraud schemes. The tools discussed above are all essential tools to address these potential fraud risks. Management can reduce fraud risk (and therefore reduce exposure to money laundering opportunities) in these areas even further by combining these tools with education for employees and customers explaining how to identify occurrences of these types of fraud, as well as potential fraud and money laundering red flags. The risk assessment processes should also help drive the overall compliance program of a digital bank which creates a guide for managing these types of risks.

Conclusion

Digital banks saw an opportunity to revolutionize an archaic industry, and as a result are gaining massive traction. Unfortunately, fraudsters have joined their mass of customers and are constantly innovating to bypass fraud detection solutions.

As digital banks work to establish their reputation amongst customers, investors, and partners, it is vital that they take a serious approach toward fraud. Implementation of an appropriate fraud risk assessment, fraud prevention program, and promotion of fraud awareness through all facets of a digital bank will help reduce the potential loss exposure resulting from fraud.

By using cutting-edge technology and a collaborative approach, digital banks can protect their top line and avoid major fraud losses, compliance headaches, and government fines.

FIVERITY

FiVerity provides financial institutions with the industry's first holistic approach to digital fraud defense. The platform integrates with a range of fraud detection solutions and data sets to deliver a comprehensive view of the threats facing an organization, with a layer of intelligence that provides actionable insights.

To find out more about how FiVerity can help you manage fraud and grow with confidence, visit fiverity.com or email info@fiverity.com.

FiVerity / 361 Newbury St / Boston / MA / 02115