feedzai

Financial Crime Report

Q1 2021 Edition

OVERVIEW

A Tale of Two Pandemics

The year 2020 was the best of times — if you're a fraudster. For the rest of us, it was the worst of times. The tale of two pandemics is one of fraudsters rejoicing at the rapid shift to digital banking and commerce, and one of consumers getting swindled by purchase, impersonation, money mule schemes, and account takeover (ATO) scams.

Feedzai's exclusive data comparing Q4 2020 vs. Q1 2020 shows:

650%

Increase in ATO scams

250%

Increase in online banking fraud attacks

178%

Fraud rate increase for digital media

70%

of all fraud is driven by **card not present (CNP) transactions**

48%

Drop in card present (CP) fraud attacks, though transaction volume only drops 20%

The Financial Crime Landscape

When it comes to the pandemic, we're all in this together – just not at the same time.

The pandemic's impact varies widely across regions and timelines. Feedzai's data from financial transactions across the world shows a stark difference in consumer behavior and financial crime in the Asia-Pacific (APAC) region as compared to Europe (EU) and North America (NA).

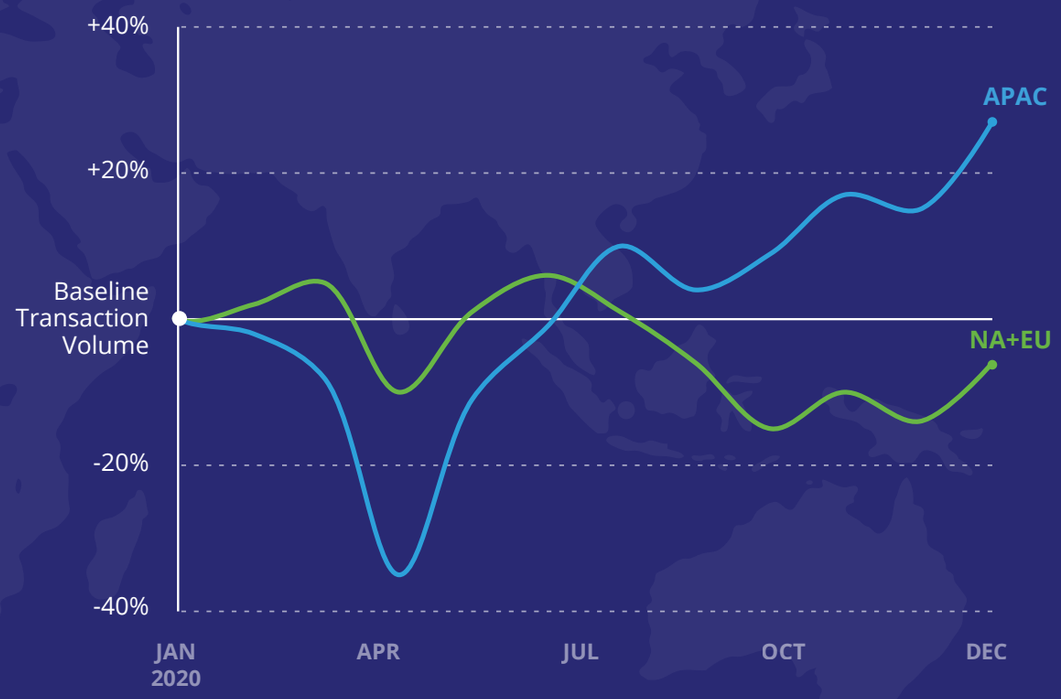
While the pandemic began in APAC, and this region saw the largest dip in economic activity early on in the crisis, the transactional volume has since recovered. That is not the case in EU or NA.

It should be noted that recovery within these large global regions does not occur at the same rate. Still, a clear image appears: a hyper-digital world where east and west are in different recovery stages - yet another tale of two pandemics.

The outlook varies by country depending on numerous factors, including COVID-19 infection rates, the effectiveness of government responses, supply chain issues, and whether business sectors rely on in-person services or global trade. We have anonymized, normalized, and generalized our data.

APAC Recovers While North America and EU Fall Behind

Variation of monthly transaction volumes between APAC and NA + EU



650% Increase in Account Takeover Scams in Q4

Transfers occur when consumers move money from one account to another. The growing popularity of real-time payment functions, combined with the expansion of online banking, means that money moves quickly, and once it's gone, it's almost impossible to get back. This fact makes the radical rise in transfers fraud scams, particularly ATO scams, all the more painful.

Feedzai's fraud experts noticed an uptick of stolen credentials for sale on the dark web in 2020. The proliferation of stolen credentials, along with the exponential rise in online transactions, provided ideal conditions for fraudsters to blend in with legitimate consumer traffic without being detected. As a result, fraud surged in the third and fourth quarters. The surge in ATO fraud caused the Q4 spike in internet banking seen in the graph.

650%

Increase in ATO Scams

600%

Increase in Impersonation Scams

300%

Increase in Purchase Scams

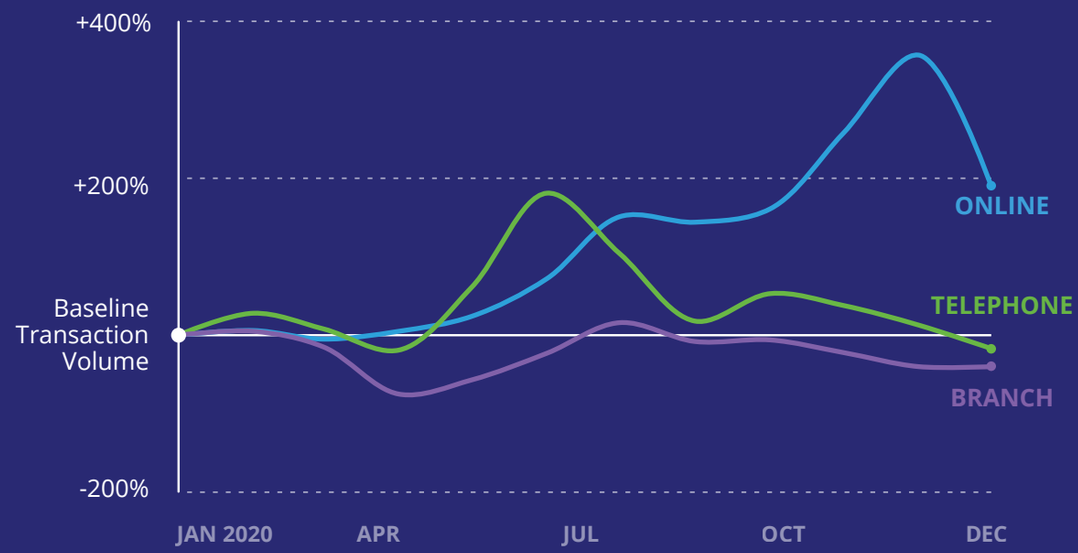
250% Increase in Online Banking Fraud

Online banking isn't new, but it's newly popular. There's been a 200% increase in mobile banking, and fraudsters worked to blend in among them. Online banking experienced a 250% increase in attempted fraud.

As expected, both telephone and branch fraud rates dropped to lower levels than they had been before the pandemic.

Fraud Volume in Banking

Monthly variation in fraud volumes between branch, telephone, and online banking



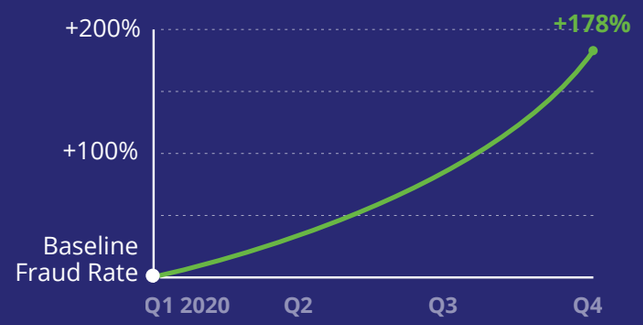
178% Fraud Rate Increase for Digital Media

In Q2, during the height of global lockdowns, demand for books and streaming services such as music and movies increased. Demand remained strong in the APAC region, but NA and EU eventually returned to pre-pandemic baseline levels.

The story around fraud is quite different, at least for NA and EU. Fraud attacks increased a whopping 178% since January 2020.

Fraud Rates in Digital Media

Percent change in NA and EU



CNP Transactions Drive 70% of Fraud Attacks

Fraudsters know a gift horse when they see one; the sheer number of online transactions provides cover to commit crime. Victims, who are themselves transacting more than ever before, might not notice a suspicious or unfamiliar transaction until months pass by. By the time they report the problem, the fraudster has moved on to the next stolen credential. Fraudsters love CNP transactions, and without essential security measures such as machine learning, behavioral analytics, biometrics, and two-factor authentication (2FA), they likely will for some time to come.

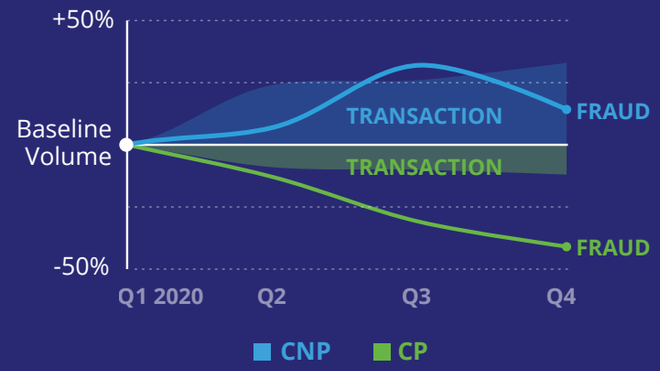
48% Drop in Card Present Fraud Attacks; Volume Only Drops 20%

Are fraudsters social distancing? It would appear so. CP transactions dropped by about 20% from the start of the pandemic and have consistently remained around that level, but fraud attacks tumbled by an incredible 48%. Perhaps fraudsters, like the rest of us, prefer contactless delivery.

Unsurprisingly, the number of CNP transactions increased by almost 35%, and fraud attacks followed suit.

CNP & CP Transaction and Fraud Volume

Percent change between Q1 and Q4 2020



The Fraud Report

The Top 5 Transfer Fraud Schemes

Across the board, the pandemic was a boon for fraudsters and a burden for consumers. When it comes to transfers fraud, criminals were more drawn to the following five fraud schemes than to all others.

1

Impersonation Scams

In impersonation scams, scammers contact consumers via email, phone, or text and claim to be from organizations such as government agencies or financial institutions (FIs). They ask the consumer to make a payment. It's possible impersonation scams worked in 2020 because people were isolated and more inclined to engage with fraudsters, along with having more time to do so.

23%

2

Purchase Scams

The pandemic uncovered supply chain vulnerabilities that created shortages of critical supplies such as N95 masks and medical equipment. Never one to miss a money-making opportunity, fraudsters built fake eCommerce sites selling anything and everything that was in short supply. Unsuspecting victims paid for goods that never arrived.

22%

3

Account Takeover Scams

In an ATO attack, fraudsters obtain stolen credentials, account information, and passwords that belong to legitimate users. Once they access the account, they can transfer funds or buy goods with stolen credentials.

22%

4

Investment Scams

Investment scams often prey on desperate people, which makes a pandemic a gold mine for fraudsters. Investment scams include employment scams, affinity fraud, pyramid schemes, and Ponzi schemes. Whatever the ruse, investment scams offer unrealistic opportunities at a cost that will never be worth the price paid.

6%

5

Romance Scams

In a romance scam, a fraudster pretends to be romantically interested in an unsuspecting victim. The fraudster will often exploit their target's emotions and manipulate them into giving the fraudster money or buying them valuable items.

3%

Top 5 Global Industries Targeted for Debit and Credit Card Fraud Attacks

Fraud $ Amount

1. **ATMs**
2. **Grocery Stores**
3. **Money-related Services** not provided by FIs (e.g., cryptocurrency, money orders, etc.)
4. **Computers and Software Stores**
5. **Specialty Retail Stores**

Fraud Rate

1. **Subscription Services**
2. **Real Estate Rentals**
3. **Money Transfers**
4. **Digital Media**
5. **Advertising Services**

A Tale of Two Pandemics:

Consumer & Fraudster Behaviors by Industry

The following pages show industry analysis of data from NA, APAC, and EU. We compared transaction volumes and fraud attack rates using January 2020 as the baseline.

feedzai

41% Drop in Restaurant Transactions for NA, EU; APAC Up 33%

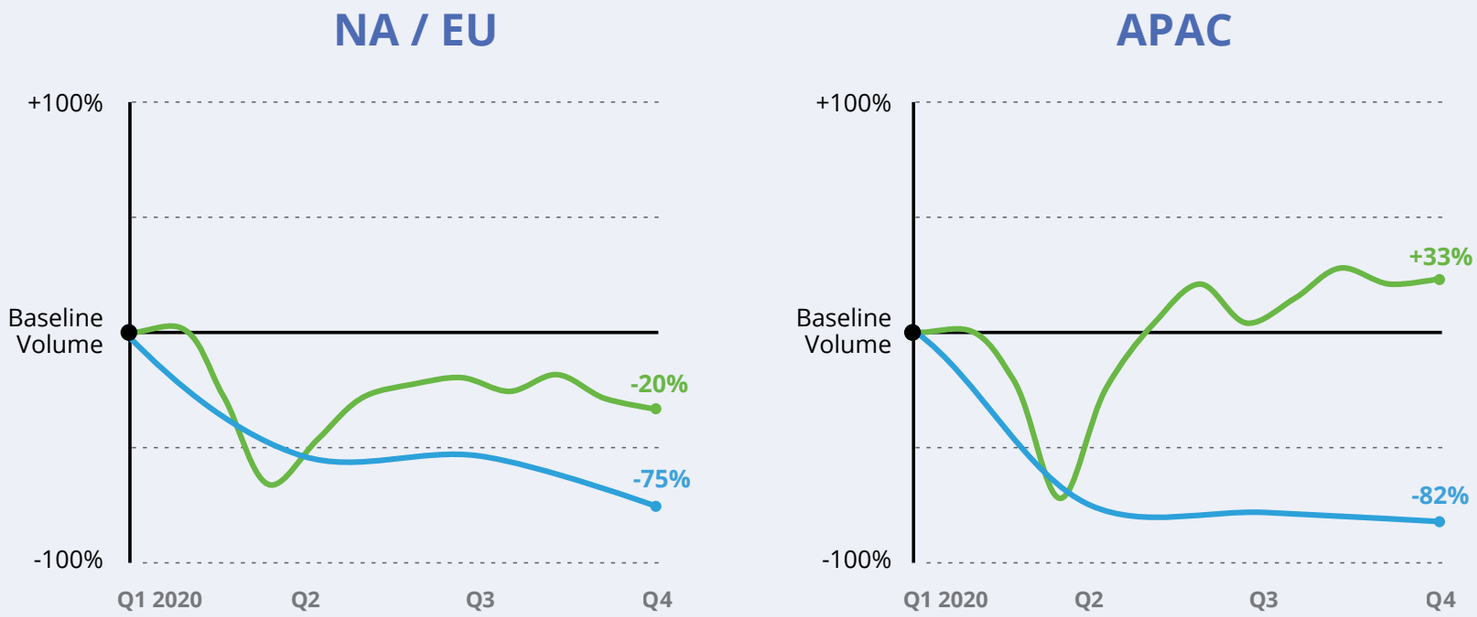
Restaurants serve a greater purpose than simply serving food. They provide social connection and economic stability. The restaurant industry was projected to employ about 1 in 10 U.S. workers. U.S. food spending totaled $1.77 trillion, and restaurants accounted for 55% of total food expenditures as recently as 2019. A hit to the restaurant industry is a significant hit to the economy.

The good news is that the restaurant industry in NA and EU is slowly showing signs of recovery. Down 41% in Q2 from January levels, Q4 was down only 20%. In APAC, the story is even better. Restaurant transactions are up 33% comparing Q4 with January 2020.

Restaurant Transactions and Fraud

TRANSACTION VOLUME FRAUD VOLUME

Quarterly percent change from Q1 2020 in transaction volume and fraud by region



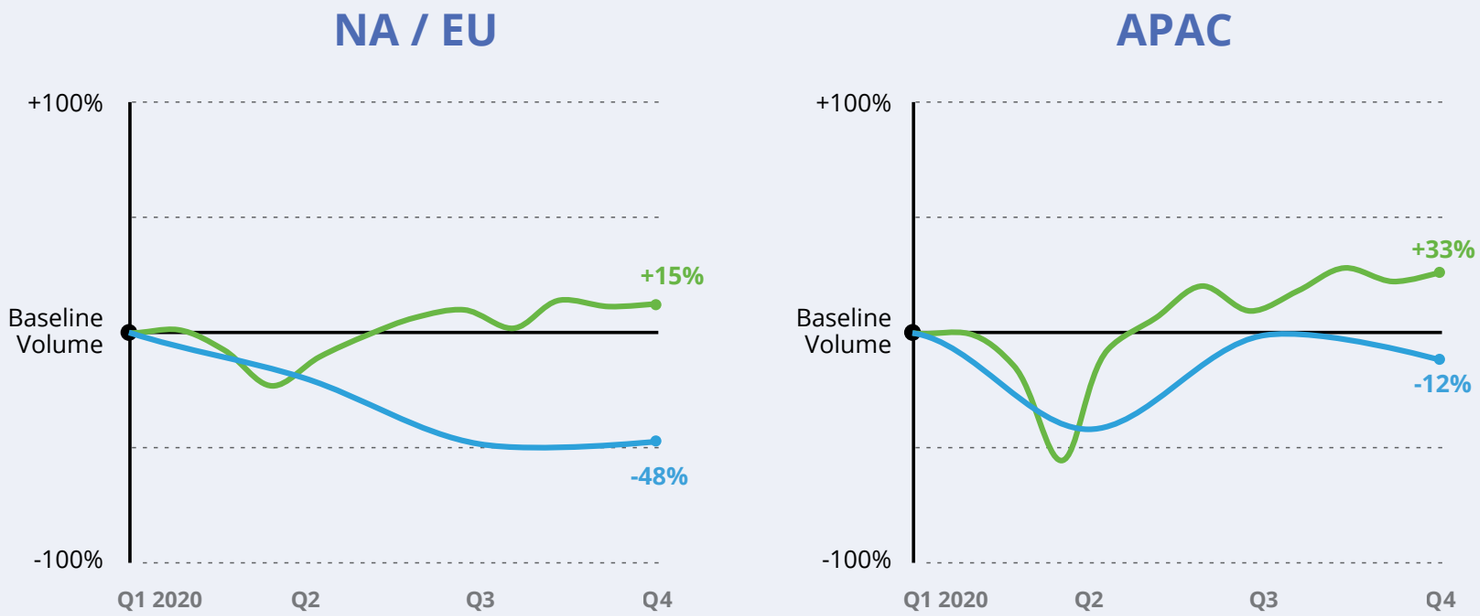
15% Increase in Fast Food Volumes; 48% Decrease in Fraud Rates

The one bright spot in the food industry is fast food. Global purchases dropped by 15% in Q2 2020 compared to January, but by Q4, purchases in Western countries were up by 15% and up 33% in APAC. And even as transaction levels surpass pre-pandemic volumes, fraud rates remain low. Perhaps fraudsters crave steak and champagne more than hamburgers and soda.

Fast Food Transactions and Fraud

TRANSACTION VOLUME FRAUD VOLUME

Quarterly percent change from Q1 2020 in transaction volume and fraud by region



13% Drop in Grocery Transactions; 51% Increase in Fraud Attack Rates

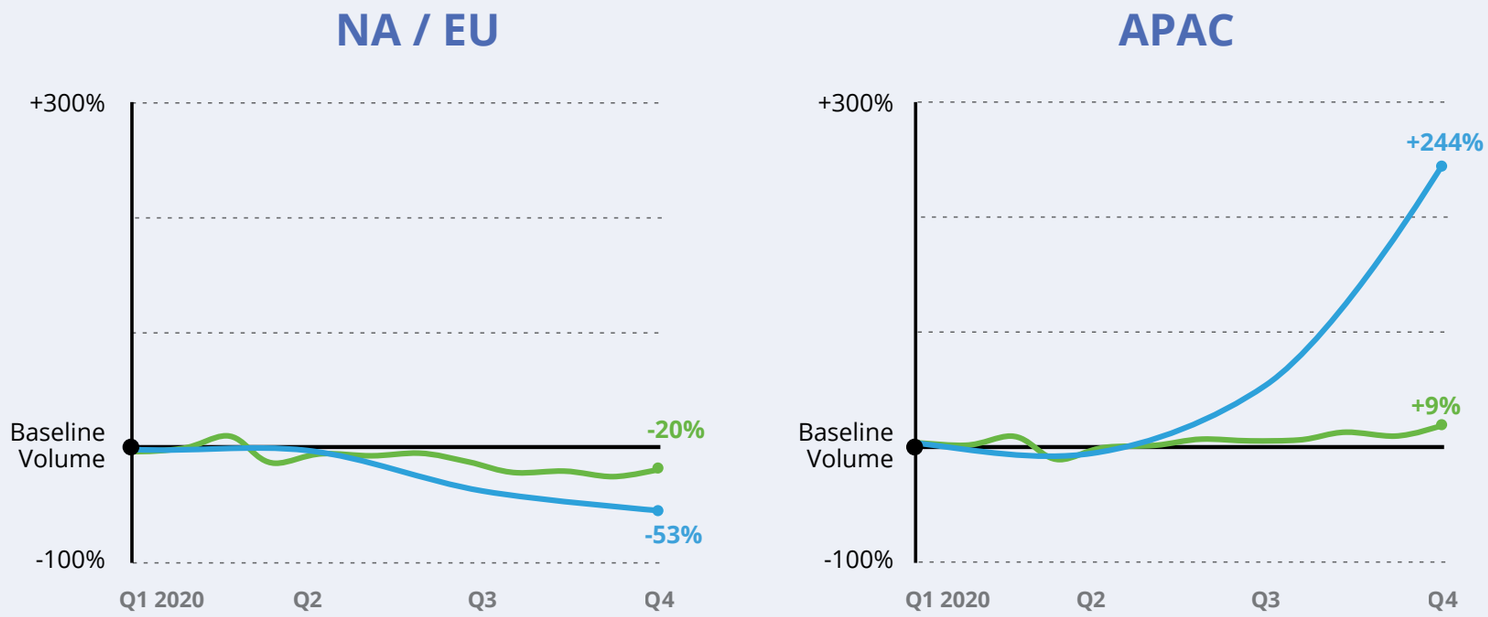
Grocery shopping is undergoing a significant change: consumers are ordering groceries online and having them delivered. Moreover, consumers are consolidating their shopping trips. Because of this, we see that the number of transactions has dipped, but the dollar amount of each transaction may be higher.

Our NA and EU data is primarily from CP transactions, which is why we see a decrease in attempted fraud. APAC fraud attacks have increased by 51% and reflect the switch to online shopping.

Grocery Transactions and Fraud

TRANSACTION VOLUME FRAUD VOLUME

Quarterly percent change from Q1 2020 in transaction volume and fraud by region



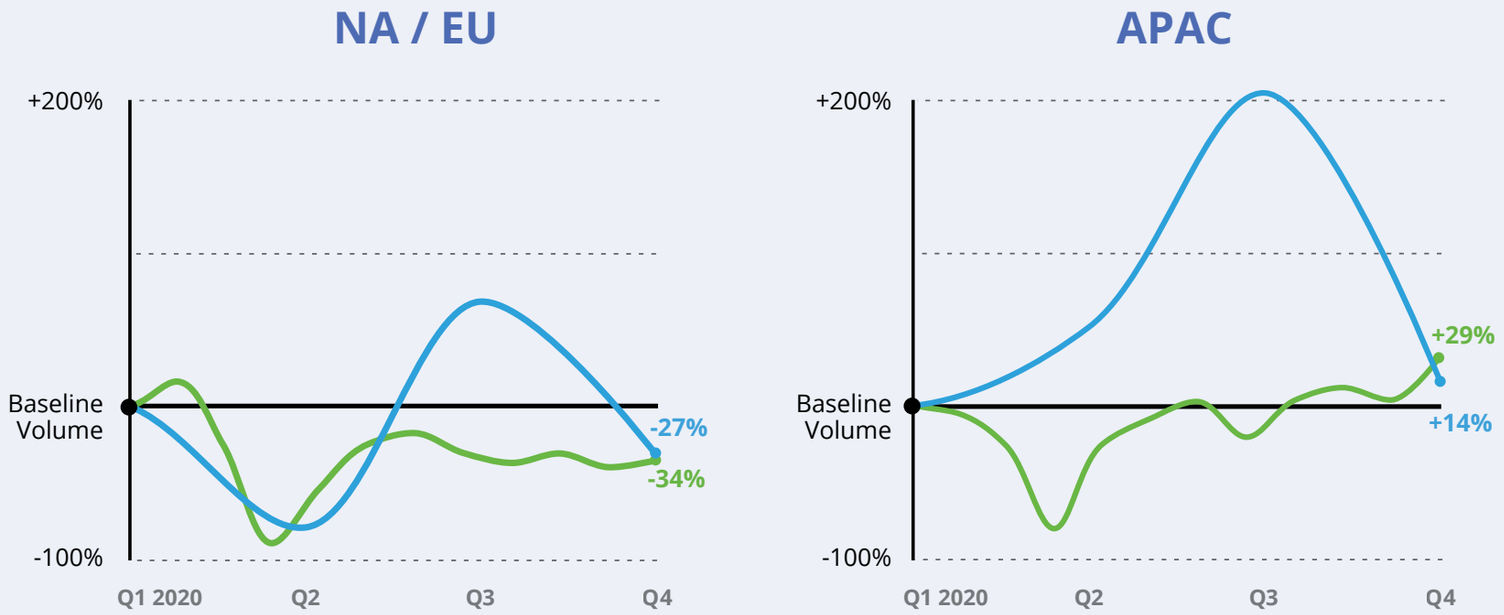
34% Cut in Beauty and Barbershops Transactions; APAC up 29%

Unfortunately, you can't get a haircut via Zoom. When governments enforce lockdowns, beauty parlors and barbershops experience drastic reductions in the number of transactions. In Q2, transactions dropped 55% in NA and EU and almost 31% in APAC. While APAC now exceeds pre-pandemic transaction levels by 29%, Western countries ended the year at 34% below pre-pandemic levels.

Beauty/Barber Transactions and Fraud

TRANSACTION VOLUME FRAUD VOLUME

Quarterly percent change from Q1 2020 in transaction volume and rates by region



56% Crash in Transportation Transactions

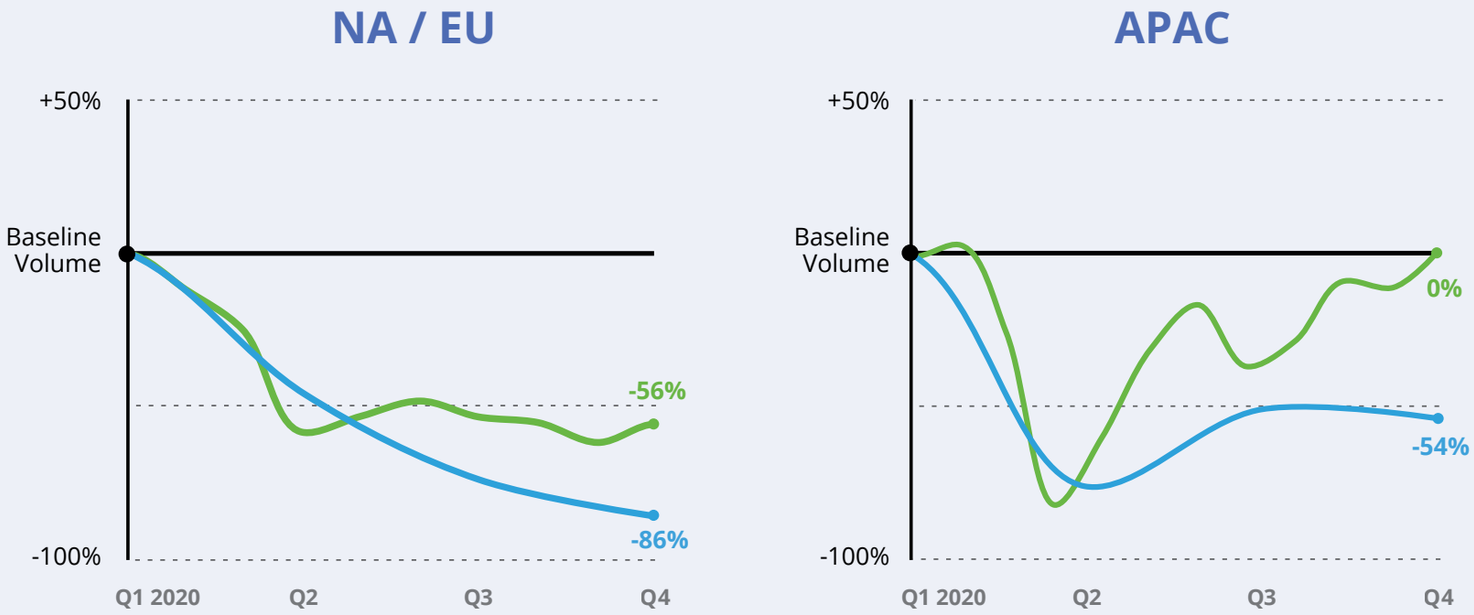
For NA and EU, the transportation industry, which includes taxis, travel, and tolls, to name a few, won't recover until people begin moving around again. Yet, it's unlikely that white-collar workers will return to the office five days a week or that we'll be as mobile as we were before the pandemic. This is one sector that even fraudsters aren't touching. Fraud rates dropped 86%.

The APAC region tells a different story. By Q4 2020, the transportation sector was largely as it had been pre-pandemic. Interestingly enough, fraud rates remained 54% below January 2020 numbers.

Transportation Transactions and Fraud

TRANSACTION VOLUME FRAUD VOLUME

Quarterly percent change from Q1 2020 in transaction volume and fraud by region



24% Drop in Gas Demand; Stable in APAC

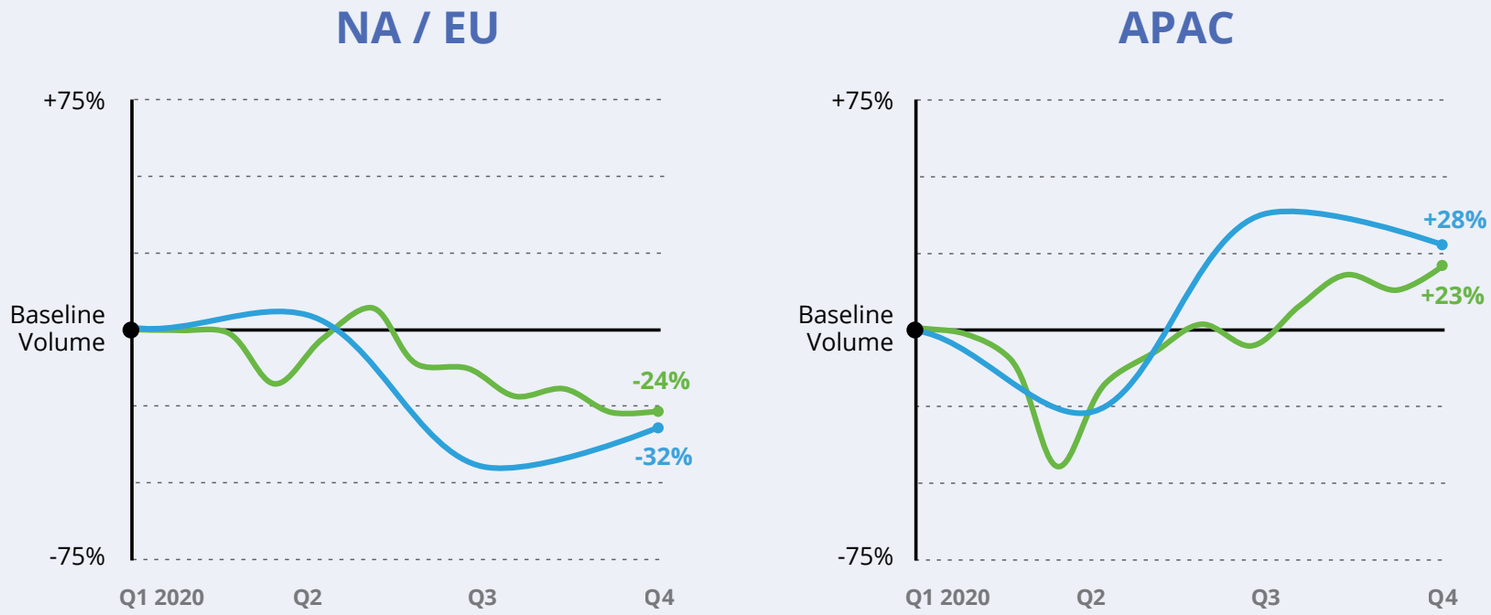
Despite a short-lived return to normalcy at the gas pumps in June, demand for gas in NA and EU continues to decline. In addition to the gas and tangential industries, states and regions that budget for taxes generated by gasoline purchases will continue to experience shortfalls through at least the first half of 2021.

The story is quite different in APAC. Gas purchases exceeded pre-pandemic levels, starkly illustrating the tale of two pandemics.

Gas Transactions and Fraud

TRANSACTION VOLUME FRAUD VOLUME

Quarterly percent change from Q1 2020 in transaction volume and fraud by region



56% Increase in Electronics and Software Purchases in APAC; 16% Increase in Fraud Rates

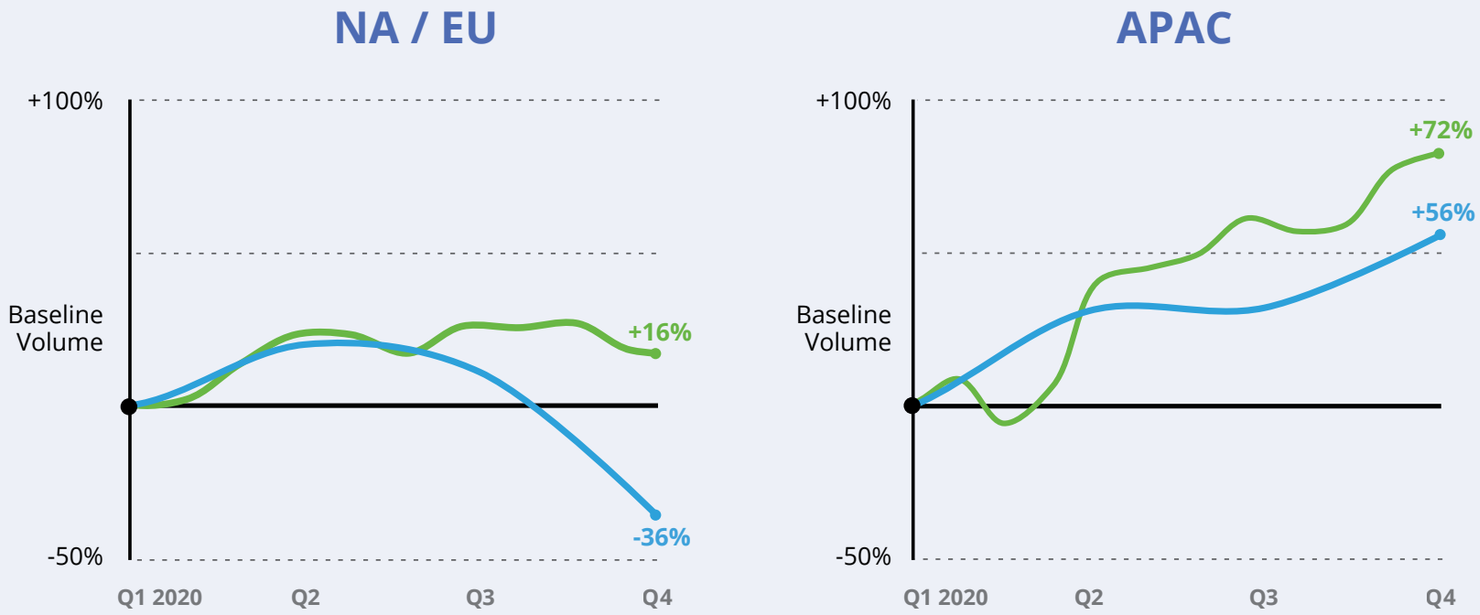
Due to lockdowns and social distancing requirements, consumers working from home or otherwise homebound looked to electronics for connection, communication, and entertainment. Electronic and software purchases increased by 16% in NA and EU, with a 72% increase in fraud rates.

Recovery is even more remarkable in the APAC region, which closed the year with a 72% increase in electronic and software purchases. Of course, fraudsters tagged along, driving the fraud rate up.

Electronics Transactions and Fraud

TRANSACTION VOLUME FRAUD VOLUME

Quarterly percent change from Q1 2020 in transaction volume and fraud by region



Anti-Money Laundering (AML) Report

Economic uncertainty, a rapid shift to digitization, and high unemployment rates are the best of times for money launderers, particularly those who organize and recruit money mules. In 2020, the FBI took action against 2,300 money mules, an increase of 383% from 2019. Of course, it's impossible to know how much crime occurs. Still, the United Nations Office on Drugs and Crime estimates that the annual amount of money laundered globally is in the range of $800 billion and $2 trillion US dollars.

Top 5 AML Red Flags

AML alerts don't necessarily mean a crime occurred. FIs determine their risk thresholds and sets their alerts accordingly. However, several triggered AML alert types can indicate that money mules are funneling money obtained through illegal activities.

1 

Rapid Movement of Funds

Transferring a specific amount into an account and then quickly moving it back out triggered the most AML alerts.

2 

Transactions in Same or Similar Amounts

This alert triggers when we see a specific amount deposited into an account and then see that same amount withdrawn or transferred out.

3 

High-Risk Geography

The Financial Action Task Force (FATF), the global money laundering and terrorist financing watchdog, provides lists of jurisdictions with strategic AML deficiencies and high-risk jurisdictions. Activity from accounts in these jurisdictions often triggers alerts.

4 

Activity in Dormant Account

Money launderers open accounts, deposit illicit funds, conduct a small number of transactions to test the system, and then leave the account idle until they are ready to launder money. The time the account remains unused can be months or years. Once the account becomes active after a period of inactivity, an alert triggers. In a risk-based approach, every FI determines how long an account can be idle before sudden activity triggers an alert.

5 

Transactions in Round Amounts

Known as "structuring" or "smurfing," transactions in round amounts are common red flags for money laundering. This tactic evades monitoring and reporting thresholds. By "structuring" money deposits into smaller, rounded denominations, criminals are less likely to trigger alarms. Also, banks and other FIs are required to file suspicious activity reports (SARs) when transfer activity reaches a set limit (usually $10,000), so criminals will structure their deposits, withdrawals, and transfers below reporting thresholds to avoid detection. The majority of legitimate transactions do not have trailing zeros (e.g., $1,000.00). Monitoring transactions with trailing zeros at the account level can detect fraudulent activity, particularly when combined with other alert triggers.

10 Financial Crime Prevention Tips for Consumers

Fraudsters are eager to separate you from your money. Here are some tips to keep your finances secure.

1 **Research**
Research retailers before you purchase and only shop on secure sites that use “https.”

2 **Use Credit Card**
Pay with your credit card, not a debit card, and enable 2FA for all online transactions.

3 **Too Good to Be True?**
If a deal is too good to be true, it’s probably a scam. This is also true for jobs promising easy money for little or no effort.

4 **Typo Alert**
Check for typos or unusual URLs in the sender’s email address, such as “service@gmil.com.

5 **Don’t Get Personal**
Avoid links that ask you to click on them to provide personally identifiable information (PII) such as social security or account numbers.

6 **Scam Calls**
Do not answer calls from unfamiliar or unknown caller IDs.

7 **Passwords**
If your credentials are stolen or compromised, change all of your passwords and never use the stolen password again.

8 **Speaking of Passwords...**
Make sure to choose complex, unique passwords for each account, and change your passwords every few months.

9 **Your Bank Won’t Call You**
Do not provide PII to anyone claiming to be a government official or from your bank; these entities will not call you and ask for this information.

10 **Transferring Money**
Legitimate employers won’t ask employees to transfer money in and out of personal accounts.

7 Ways FIs Can Prevent and Detect Financial Crime

Banks have a role to play in keeping their customers safe from fraudsters and scammers. Here are a few steps banks can take to ensure their customers are well-protected.

1 – – – – 2 – – – – 3 – – – – 4 – – – – 5 – – – – 6 – – – – 7

Create
detailed customer behavior profiles so that you can recognize and differentiate authentic customer behavior from criminal behavior.

Educate
your customers in best practices for good digital hygiene.

Implement
security measures (e.g., 2FA).

Combine
inbound and outbound payments monitoring and including movement of payments between account rings.

Capitalize
on existing relationships with e-crime providers, dark web experts, and internal and external cybersecurity professionals to uncover credential testing and check customer scam reporting.

Participate
in consortium data at least twice a week.

Leverage
rules, machine learning, and data analytics to detect and prevent fraud and financial crime.

Conclusion

There were two pandemics in 2020 – one for fraudsters and one for the rest of us. It was a good year for fraudsters.

The large volume of CNP transactions was a boon for criminals in 2020, and we expect this to continue well into 2021. ATO attacks spiked in the fourth quarter, and all indications are that they will plague us for the foreseeable future. Along with ATO attacks, impersonation and purchase scams were the most popular attack types for transfer fraud. Banks would do well to educate their customers and shore up their systems to combat these schemes, particularly in light of the 250% increase in online banking fraud attacks, by far the most utilized form of banking today.

As we move forward, anticipate the growth of money mules. Prevent and mitigate their crimes by ensuring proper account opening workflows and solutions are in place.

Fighting fraud and financial crime in a post-pandemic world is complex work. It's critical to develop technology partnerships that grow customer satisfaction while frustrating fraudsters at every crooked turn.

Methodology

The Financial Crime Report Q1 2021 Edition captures Feedzai's exclusive data from over 11 billion global transactions across all major industries for the year 2020.

Feedzai's mission is to keep banking and commerce safe. The purpose of the report is to provide valuable insights for financial institutions.

feedzai

One Platform to Manage Financial Crime

Feedzai's AI stays ahead of emerging financial crime and money laundering patterns and mitigates even the most deceptive criminals so that banks, issuers, acquirers, and merchants can focus on growth.

Feedzai is considered best in class by Aite and one of the most successful AI companies by Forbes. The world's largest banks, processors, and retailers use Feedzai's fraud and financial crime prevention products to safeguard trillions of dollars and manage risk while improving customer experience.

Account Opening | Anti-Money Laundering | Transaction Fraud

feedzai.com **sales@feedzai.com** **info@feedzai.com**