feedzai

The RiskOps Age

Q2 2022 Financial Crime Report

Overview

The year 2021 was no ordinary year. We celebrated the power of vaccines and lamented the proliferation of variants. We saw billionaires rocket into space, and the Ever Given disrupt supply chains. And we saw fraud. Lots of it.

Feedzai's exclusive data from over 18 billion transactions demonstrates that the pandemic-driven shift to online shopping and banking is likely here to stay. And this shift to digital provides tremendous opportunities to commit financial crime. Legitimate online transactions grew exponentially, but online fraud attempts grew at an even faster rate.

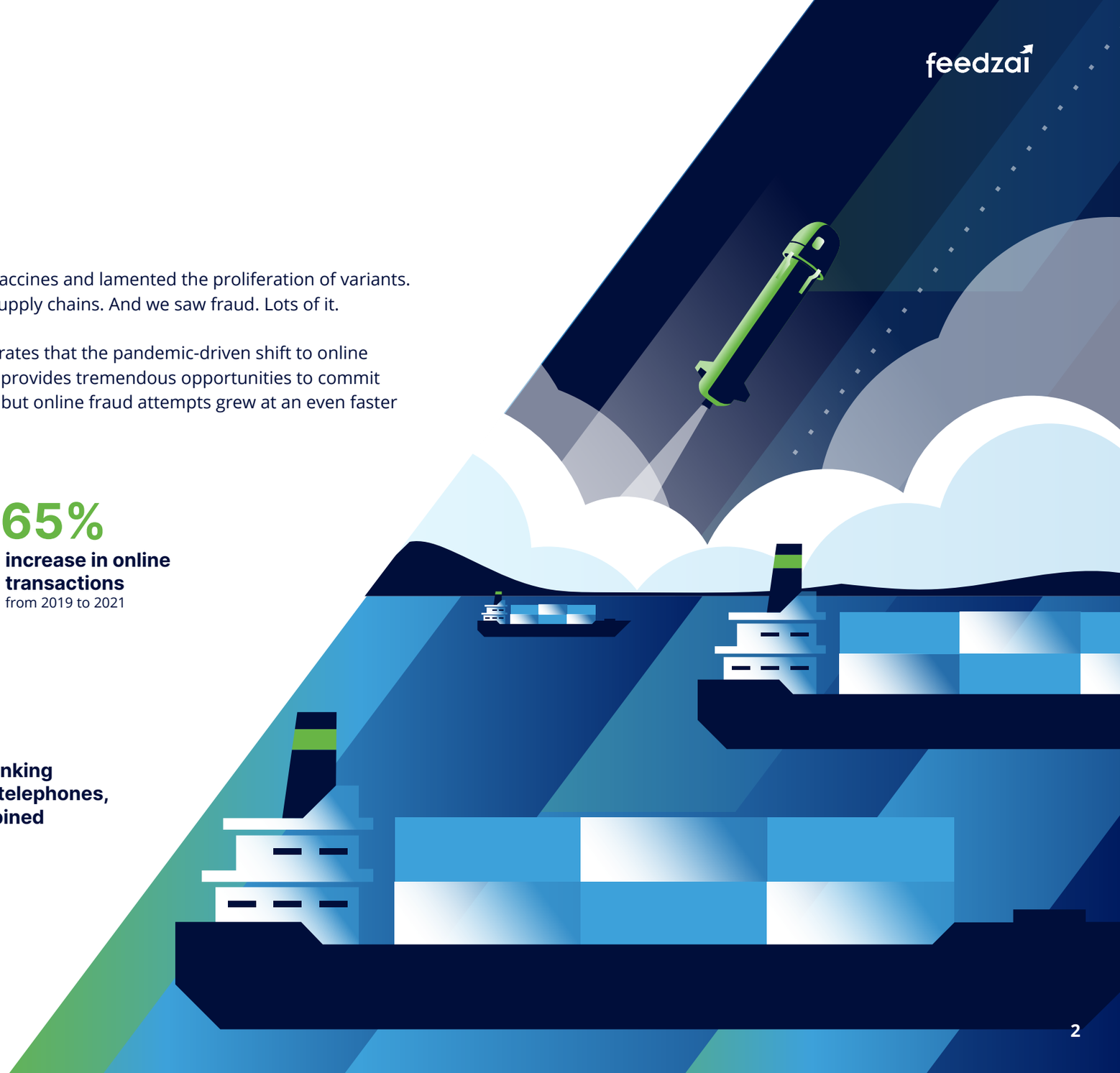
794%
increase in fraud for digital entertainment transactions
from 2019 to 2021

233%
increase in fraud attack rates
from 2019 to 2021

65%
increase in online transactions
from 2019 to 2021

75%
decrease in US cash withdrawals
comparing 2019 to 2021

+50%
lower fraud rate in mobile banking applications vs. computers, telephones, and in-person banking combined
in the UK



The RiskOps Landscape

“Online” isn’t a place or activity; it’s how we live. Each digital transaction creates multiple data points. Customers now expect banks to use their data to provide personalized offerings and experiences in real time.

Every data point is an opportunity to commit or prevent fraud. This has always been true, but never at this scale. We’ve seen exponential growth in digital transactions with real-time expectations, and there is no going back; the genie is out of the bottle.

The average American has access to more than 10 connected devices in their household. It’s common for people to have a few social media profiles per platform, possess accounts with several financial institutions, and work on multiple computers. We not only have each person transacting digitally, but we also have them doing so from a plethora of devices and accounts. We’re drowning in data.

Now imagine when much of the developed world lives in smart homes with connected refrigerators, lights, doorbells. Imagine paying for a drive-thru with your car. Imagine the metaverse.

And in financial services, we’re just starting to scratch the surface of non-fiat currency.

Without a new approach, we face the perfect storm for fraud and financial crime:

1
Customers expect **real-time payment** transactions.

2
FIs must **vet the identity** of their customers regardless of how many devices or accounts they use, and all without ever meeting them in person.

3
Fraud and financial crime teams are **distributed.**

4
Non-fiat currency has arrived.

From a fraudster's point of view, it's the best case scenario. For risk teams, it's a tipping point. The year 2021 ushered in the age of RiskOps. Now is the time to fundamentally change how organizations manage the risk of fraud and financial crime to thrive in the coming years.

Every successful retailer and bank must accept that their online transaction volume will more than quadruple in the future. This will happen faster than their current methods can manage. That's why now is the time to connect teams, connect data, and connect risk. Hire the right people, create the right processes, and use the most advanced technology to safeguard the business you have today, and the business you build tomorrow.

30%
of attempted transactions were fraudulent over 2 months
(card not present fraud)

4,000
social engineering attacks in 10 days
(online banking fraud)

+5M
cards tested over 4 months
(BIN attack)

In 2021, we saw focused attacks on major organizations' digital transactions.

+233%

Digital Commerce Delights Criminals

The biggest story of 2021 was the substantial increase in online fraud attacks. We see a drastic rise from 2019 to 2020 to 2021. While online transactions increased by an impressive 65%, this number is dwarfed by online fraud attacks, which grew 233% from 2019 through 2021. This is a trend we expect to continue.

65%
increase in online transactions

233%
increase in fraud for online transactions

+794%

Fraudsters Binge on Digital Entertainment

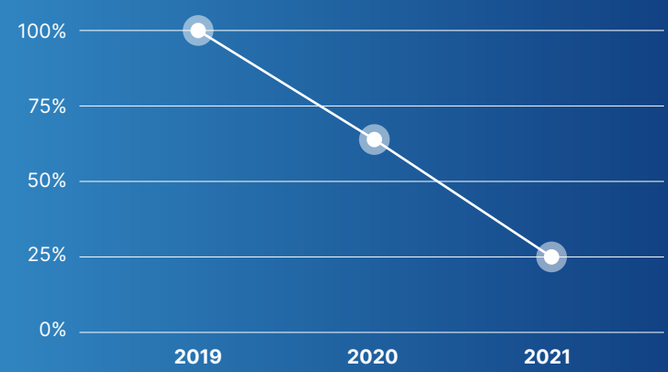
Consumers weren't the only ones binging on digital entertainment; fraudsters were too. Criminals like to hide in plain sight, and the sheer number of transactions for digital entertainment combined with the low dollar amount per transaction provides fraudsters with an ideal environment to test stolen cards along with other scams. We saw a 794% increase in fraud attacks from 2019 through 2021.

-75%

Cash is Not King in the US

In our previous Financial Crime Report, we focused on the trend away from cash. Now we see that cash didn't bounce back even when many pandemic-related restrictions were lifted. In fact, we saw a steeper decline in U.S. cash withdrawals comparing 2021 to 2020 vs. 2019 to 2020. Overall, U.S. cash withdrawals have decreased 75% from pre-pandemic levels to now.

Number of US Cash Withdraws
Normalized to 2019

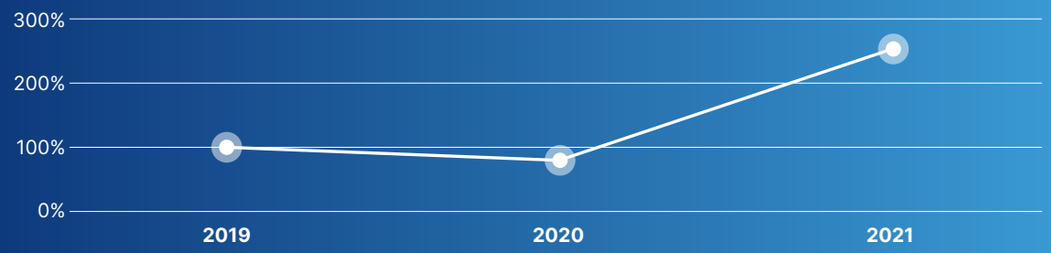


+202%

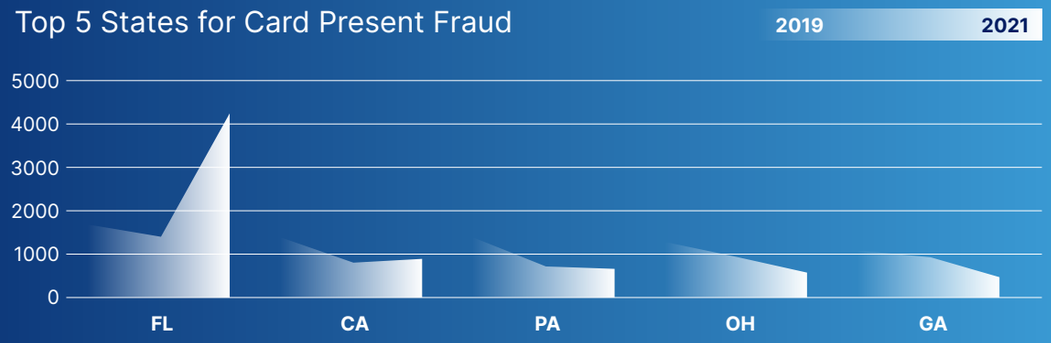
Face-to-Face Fraud in Florida

Florida takes the top spot for in-store debit card fraud. Interestingly, the number of in-store card transactions showed no significant change, making the massive spike in card-present fraud attacks particularly noteworthy. Looking at the data more closely, we see that this is not related to gas pump purchases, but rather in-store and often at 24-hour convenience stores. This shows that EMV technology is helping to curb fraud, but fraudsters are gaining access to PIN codes.

Card Present Fraud in Florida



Top 5 States for Card Present Fraud



+88%

UK Mobile Money

We might be addicted to our mobile devices, but fraudsters aren't. Fraud attacks were more than 50% more common in the UK via desktops and laptops, telephone, or in-person combined vs. mobile banking apps. Put simply, mobile banking apps are safer; consumers should be encouraged to use them.

88%
of all banking happened via a mobile device

50%
lower fraud rates in mobile banking apps

30%
higher pound (£) amount per fraudulent transaction for Android vs. iOS devices

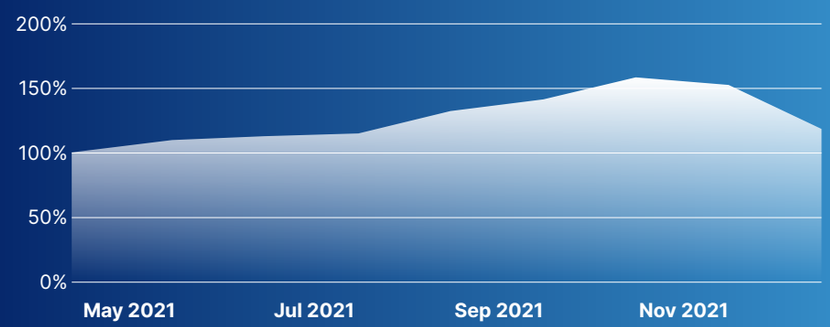
67%
higher fraud rate for iOS vs. Android device, but only 3% higher for £ fraud rate

+57%

Holidays Sparkle for P2P Payments in Brazil

Brazil's robust digital payment landscape embraced peer-to-peer (P2P) payment methods for holiday spending. We saw a steady increase from May through July and a rapid rise from July to November. Post holidays, adoption continued to be higher than the late spring period.

P2P Transactions in Brazil

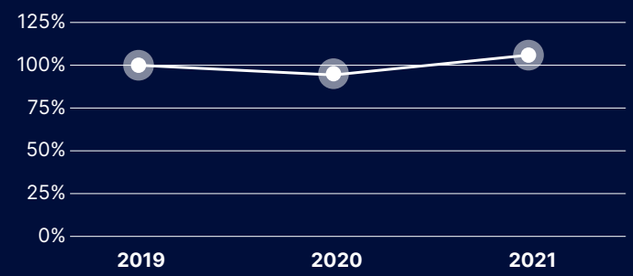


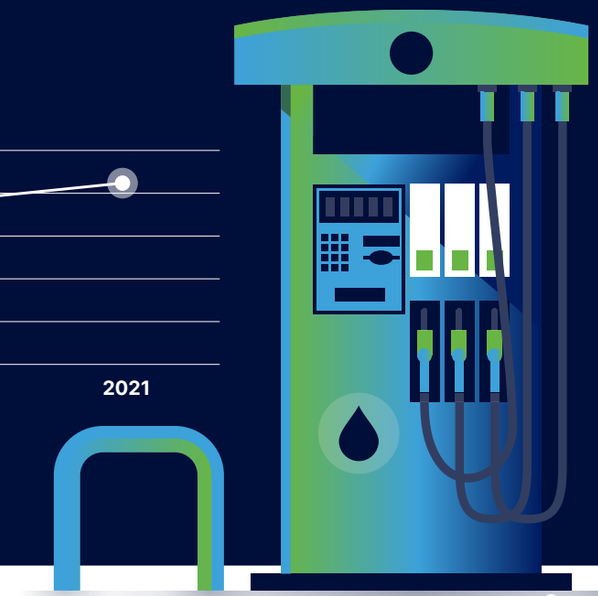
7%

Gas Increases with Inflation

Tracking perfectly with inflation, we saw U.S. gas prices increase almost 7% in 2021 compared to 2020.

Average Gas Value





Top 5 Fraud Types of 2021

1 Account Takeover (ATO)

A form of identity theft; fraudsters change account information, including passwords, and "take over" the account.

2 Social Engineering Scams

Victims are tricked into handing over personally identifiable information (PII).

3 Purchase Scams

Victims purchase goods online that never arrive.

4 Impersonation Scams

Fraudsters pretend to be legitimate actors and trick victims into compromising their accounts.

5 Smishing Scams

Text or SMS version of a phishing email.

feedzai

Top 5 Card Fraud by Merchant Categories

When it comes to card fraud, criminals know how to play the game. The online game, that is. Card fraud was highest for retailers selling online games in 2020 and 2021 in both the U.S. and Australia.

United States

In the U.S., online games and software, computer services, and money exchange services made the fraud list two years in a row. In 2021, ATM transactions and digital entertainment were replaced by gas stations and video streaming subscriptions.

2021

Online games and software	38.4%
Video streaming subscriptions	31.8%
Computer services	13.0%
Gas stations	9.0%
Foreign currency, money orders, and travelers' checks	7.8%

2020

Online games and software	40.8%
Computer services	20.6%
Foreign currency, money orders, and travelers' checks	15.8%
Digital entertainment	13.1%
ATM transactions	9.7%

Australia

In Australia, online games, miscellaneous and specialty retail stores, and dating services made the list in 2020 and 2021. However, digital entertainment and taxis replaced restaurants and computer software in 2021.

2021

Online games	31.5%
Digital entertainment	18.3%
Taxis	17.6%
Dating services	16.4%
Miscellaneous and specialty retail stores	16.2%

2020

Online games	23.4%
Miscellaneous and specialty retail stores	19.9%
Restaurants	19.7%
Computer software	18.8%
Dating services	18.3%

The United States of Fraud

Fraud Rates for Top U.S. Tourist Destinations in 2021

Fraudsters love tourist towns, and even a pandemic can't stop them. We've ranked the top six U.S. tourist cities by fraud rate and crowned Miami with the dubious honor of highest fraud rate — a title that had gone to San Francisco two years in a row. Next, we've noted the increase or decrease in fraud per city compared to 2020.

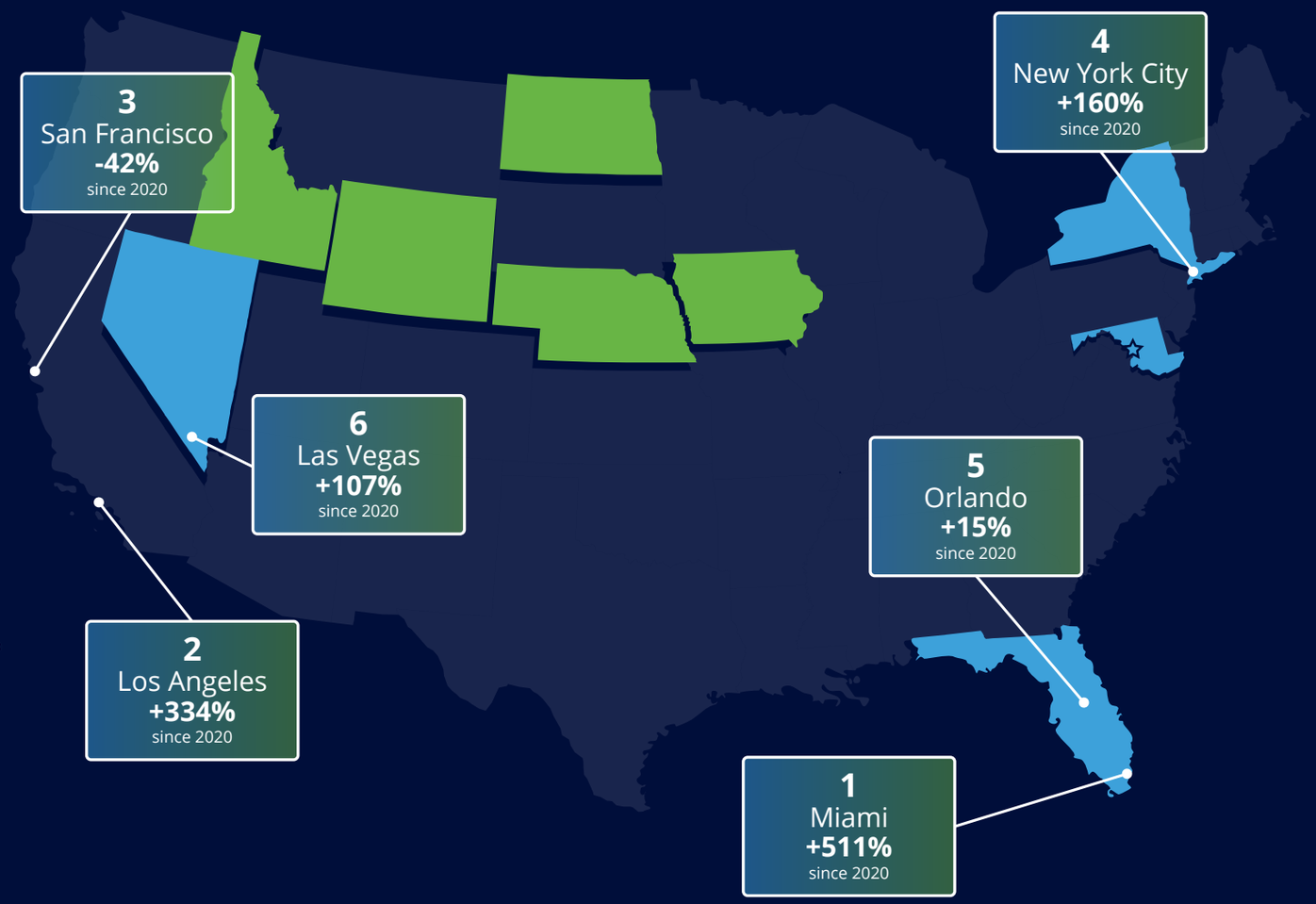
Here's a look at the rankings pre-pandemic vs. the first and second years of the pandemic.

2019

1. San Francisco
2. New York
3. Miami
4. Orlando
5. Los Angeles
6. Las Vegas

2020

1. San Francisco
2. Miami
3. New York
4. Los Angeles
5. Orlando
6. Las Vegas



States with the HIGHEST Card Present Fraud Rates in 2021

1. Florida
2. Washington, D.C.
3. New York
4. Maryland
5. Nevada

States with the LOWEST Card Present Fraud Rates in 2021

1. Nebraska
2. Iowa
3. Wyoming
4. Idaho
5. North Dakota

feedzai

The United Kingdom of Fraud

U.K. Regions with the HIGHEST Fraud Rates

1. Poole
2. Leicester
3. West Berkshire
4. Buckinghamshire
5. Derby

U.K. Regions with the LOWEST Fraud Rates

1. West Dunbartonshire
2. East Lothian
3. North Ayrshire
4. Wrexham
5. Dumfries and Galloway

feedzai

5 Ways Consumers Can Prevent Social Engineering Attacks

Scammers defraud victims by manipulating emotions such as fear, hope, or curiosity to trick them into providing personally identifiable information. Your job is not to fall for it. Here are some tips to counter social engineering attacks:

1 Remember, the click is a trick.

Don't open or click on suspicious links via email or text. Fraudsters can't trick you if you don't click on their links.

2 Update devices.

Install and regularly update anti-malware software. When your computer or phone prompts you to install updates, do it.

3 Protect your privacy.

Don't provide personal information about yourself or your employer unless you are 100% sure the person you're interacting with should have access to that information.

4 Use multi-factor authentication.

Do not reveal personal or financial information in email, and do not respond to email or text messages asking for this information. This includes clicking on links sent via email or text.

5 Don't believe the hype.

If an offer, prize, or opportunity is too good to be true, it isn't true. Don't fall for tempting out-of-this-world offers.

5 Tips for Banks to Combat Social Engineering Fraud

1 Work with other banks.

Pool your collective intelligence and agree on best practices for the industry, including who pays for losses.

2 Over-communicate with customers.

Communicate consistently with customers, and try new channels. Don't let the messaging go stale. If a TikTok dance about social engineering is how your customers will hear you, start dancing!

3 Shift from fraud detection to prevention.

Fraudsters are scaling their operations. This means banks need a new strategy. It's not enough to detect fraud anymore; you have to prevent fraud. It's time to know your user, i.e., leverage device and behavioral biometrics.

4 Be criminal-minded.

Do whatever it takes to know how a fraudster's mind works. Talk to defrauded customers; investigate scams like you're looking for the rosetta stone. Use the knowledge to understand how scams are engineered and develop new processes to thwart them.

5 Support customers.

Be empathetic with defrauded customers. They're often angry, embarrassed, and looking to blame someone. Train staff to be patient with victims and help them through the ordeal so they feel supported by the bank, and you gain essential intelligence on the scam's mechanics.

Conclusion

The payments landscape has irreversibly changed. The amount of data created by each digital transaction, the fragmentation of identity across devices and accounts, and customers' expectations of real-time transactions means financial institutions must shift their approach to fraud and financial crime risk management. We have entered the RiskOps age.

Online fraud attacks grew at a higher rate than legitimate online transactions. Digital entertainment is a particular target for fraudsters, but in-store fraud continues to be a problem. Fraudsters' current favorite schemes are ATO and social engineering attacks. The good news is that mobile banking is proving safer than online, telephone, or in-person banking; encourage customers to use it.

The pandemic has proven unpredictable, but the shift to digital commerce is here to stay. The future of money is digital, and financial institutions must secure that future today. A smart way to do this is to connect to networks that allow intelligence sharing and access to as much data as possible. In this way, financial institutions can understand and manage today's market risks while preparing for digital currencies and tomorrow's new, emerging threats.

Methodology

The *Q2 2022 Financial Crime Report: The RiskOps Age* captures Feedzai's exclusive data from over 18 billion global transactions across all major industries from 2021 unless otherwise noted.

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

feedzai

Transform Your Risk Management

Feedzai's AI stays ahead of emerging fraud and financial crime and mitigates even the most deceptive schemes 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 organizations 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