feedzai

Fraud Scam Detection:

How Feedzai Supports Fraud Scam Detection and Advises on Operational Execution

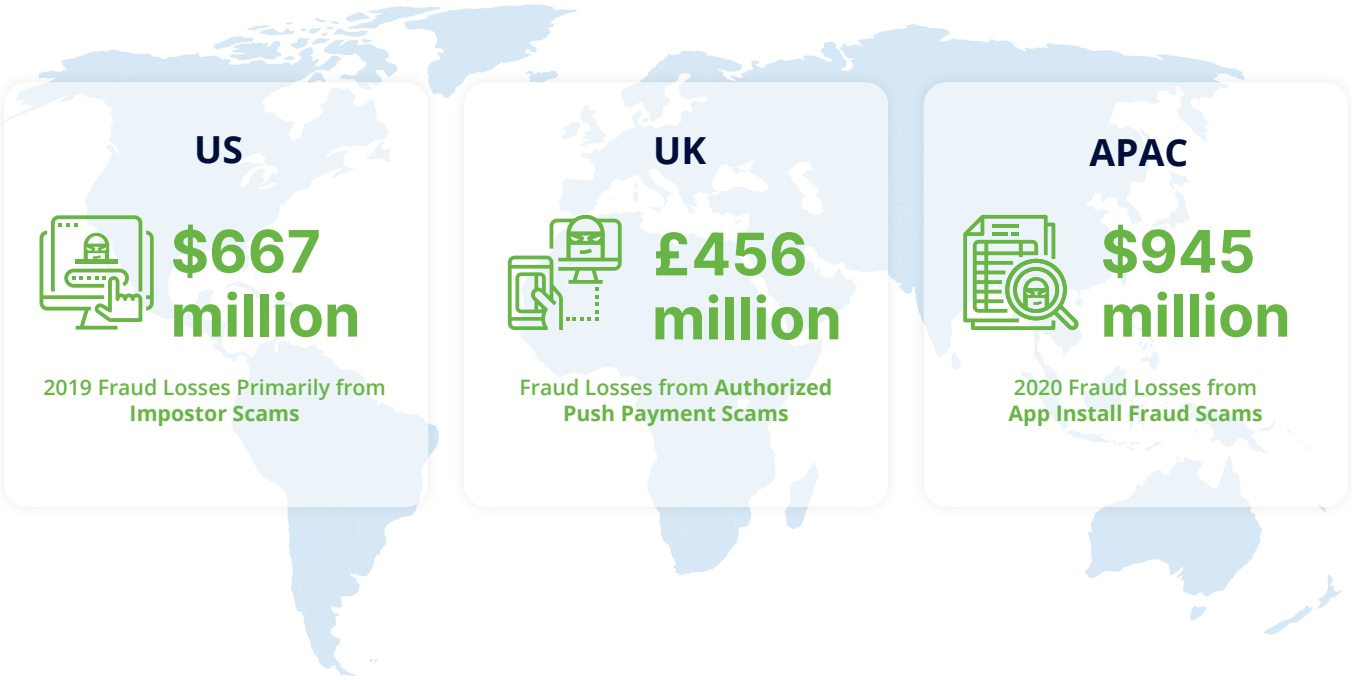
Contents

The Rising Worldwide Trend of Fraud Scams

Scam trends are alarming at a global level. The US FTC reports 2019 fraud losses at nearly $667 million, primarily as a result of impostor scams. That's a 32% increase from the previous year's $497.2 million fraud losses. UK financial markets are equally hard hit with Authorised Push Payment (APP) scams experiencing gross losses of £455.8 million. In both instances, consumers fall victim to a fraudster's lie and initiate the transaction.

APAC is a unique market where consumers are being tricked into downloading fraudulent apps and then scammed out of their money. In this region 1 in 5 app installs is fraudulent. The dollars associated with this activity is significant. AppsFlyer has estimated that the cost of app install fraud globally in the first half of 2020 was US $1.6 billion. Asia-Pacific accounts for a whopping 60% of this total figure — with the financial exposure of fraud in the region estimated to be US$945 million, up 45% from 2019's US$650 million.

Fraud Losses Worldwide



Types of Scams

Authorized Push Payment Fraud

APP fraud happens when fraudsters deceive consumers or individuals at a business to send them a payment under false pretences to a bank account controlled by the fraudster. As payments made using real-time payment schemes are irrevocable, the victims cannot reverse a payment once they realise they have been conned.

APP fraud is problematic and has been broken out into two primary categories:

Malicious Payee Fraud
The customer is tricked in buying goods and paying, but they are fake.

Malicious Misdirect Fraud
The customer makes a payment to what they think is a legitimate account but they are redirected to a mule account instead, typically SE, invoice, etc.

Funds from APP fraud are rarely recovered in most cases.

Business Email Compromise (BEC) or Email Account Compromise (EAC)

BEC is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam that targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Fraudsters have gravitated toward BEC fraud at an alarming rate. In 2019 the FBI had case totals that aggregated to a total losses of US$1.77 billion. BEC had the highest category of losses for all Internet Crime Complaint Center (IC3) investigations.

BEC Fraud

$1.77 Billion

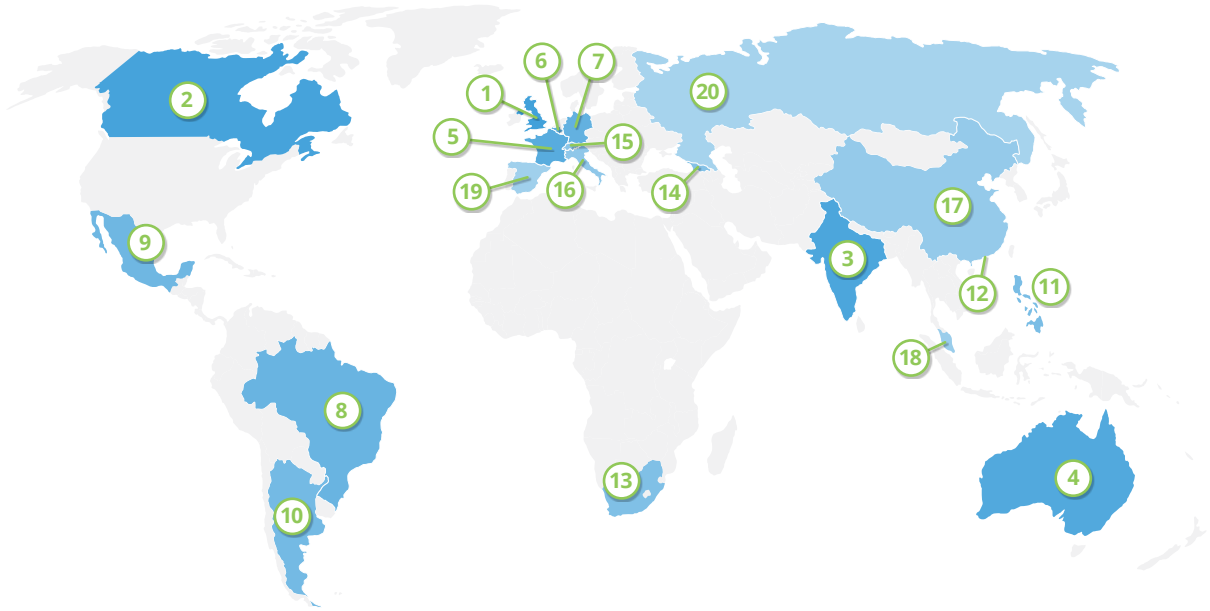
Total losses from a 2019 US Fraud Case investigated by the FBI

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 romantic interest and manipulate them into giving them money or buying valuable items on their behalf.

2019 Top 20 International Victim Countries

Exluding the US



1.	United Kingdom	93,796	11.	Phillippines	561
2.	Canada	3,721	12.	Hong Kong	535
3.	India	2,901	13.	South Africa	465
4.	Australia	1,298	14.	Georgia	454
5.	France	1,243	15.	Switzerland	438
6.	Belgium	1,031	16.	Italy	428
7.	Germany	850	17.	China	403
8.	Brazil	628	18.	Malaysia	362
9.	Mexico	605	19.	Spain	358
10.	Argentina	587	20.	Russian Federation	349

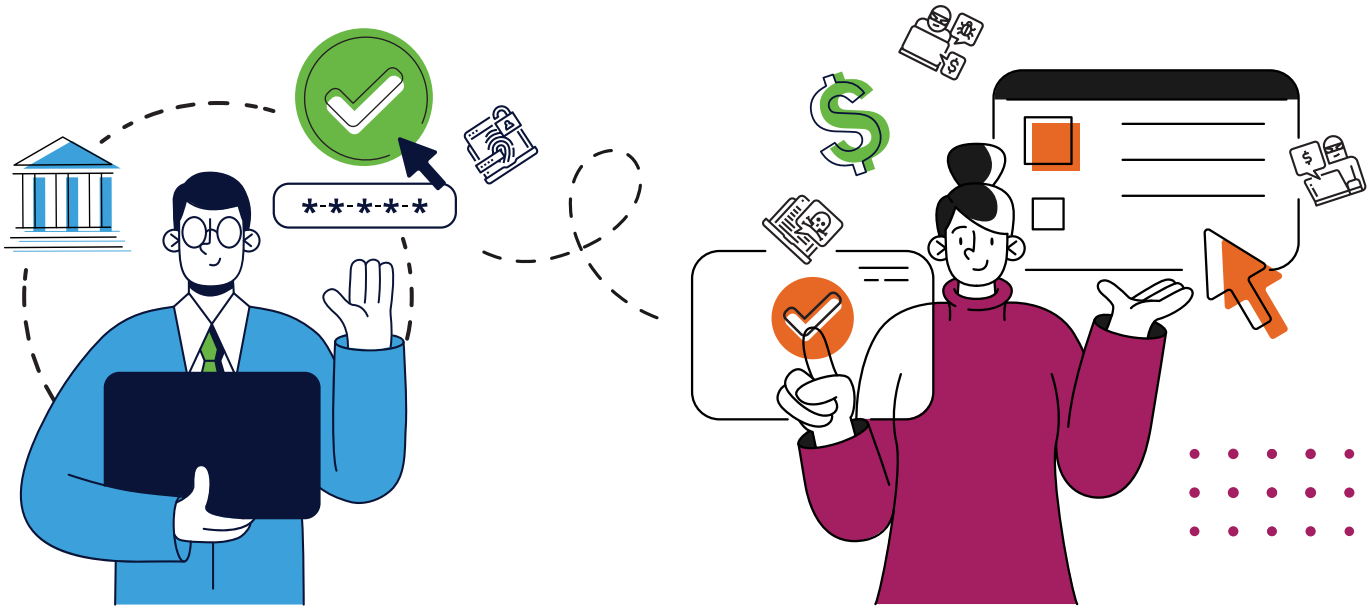
Why have scams become a bigger problem?

For years banks have been adding risk controls to curb fraud losses and make it harder for fraudsters to line their pockets with illicit funds. These risk controls range from EMV chip adoption, online banking controls, and implementation of risk solutions like Feedzai. The fraud pendulum has once again swung to the point of least resistance - in this case, to the consumer who has been tricked or duped into a scam.

It's challenging to detect the activity of a scammed victim because the consumer will tend to validate the activity they believe is legitimate and necessary to conduct the transaction.

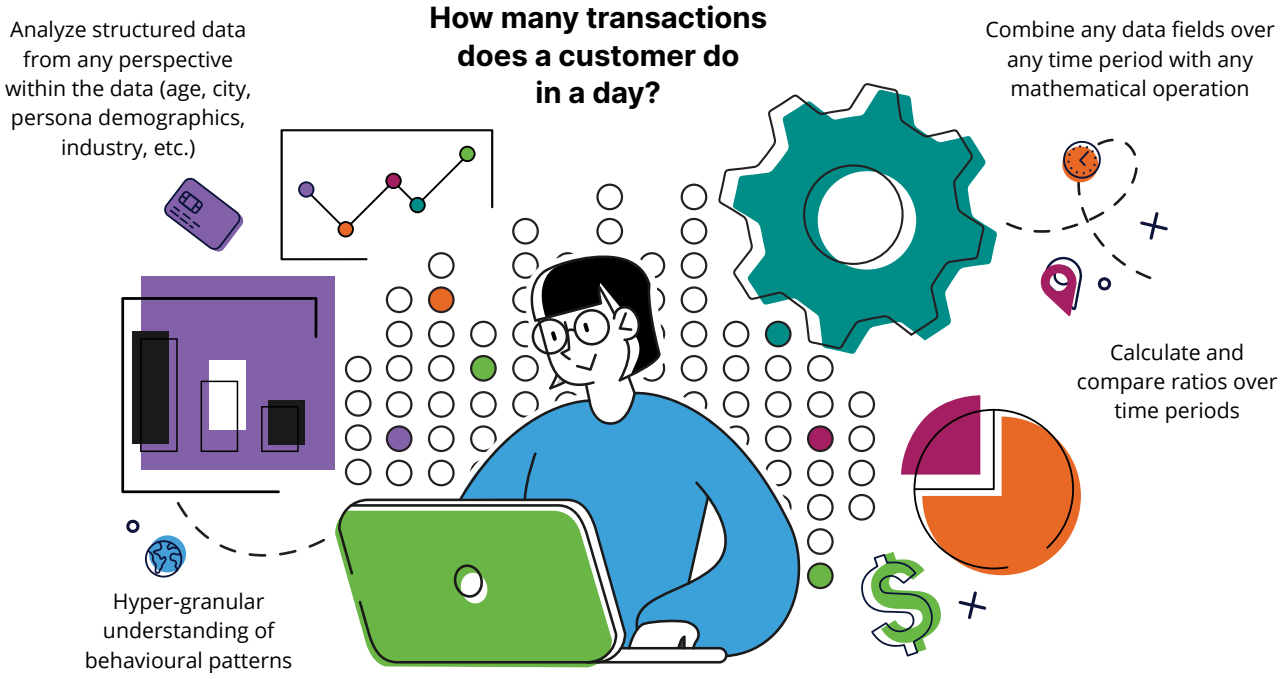
Several governments worldwide have responded to the increase in scams by enacting policies requiring FIs to reimburse scammed consumers. In the UK, for example, the Contingent Reimbursement Model places the liability of scams (losses) back to the account holder's FI. This puts an onus on the bank to further substantiate the account holder's activities.

Fraudsters have pounced on this shift in policy and liability, taking advantage of willing and unfortunately naive victims. It's common for these scams to last a long duration of time as fraudsters work to establish credibility. The ultimate goal is for the fraudster to drain their victim's pockets after they willingly validate the activity with their bank.



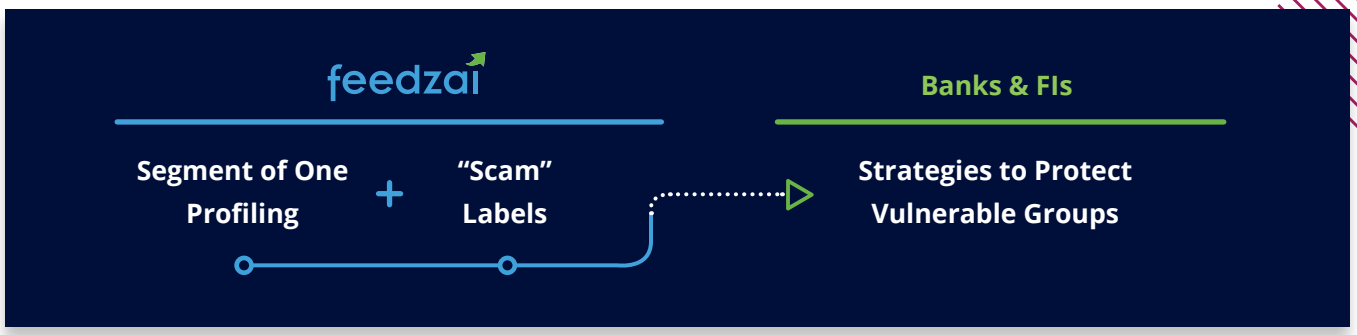
How Feedzai Detects Scams

Knowing customer behaviour is key to fighting scams, and Feedzai has the ability to measure the behaviour of data at a sub-event level. We call this **Segment of One** profiling.



Feedzai Segment of One Profiling

Creates a rich profile of a customer's genuine activity and transactions, allowing identification of scams or activity that is out of the ordinary



Scam Detection Deep-Dive

Propensity to Become a Scam Victim

Feedzai uses consumer and profile customer data to identify customers who have a higher propensity to become a scam victim even before a scam starts. Example: Profiling account balances that were previously high and in a short period of time decrease, with no payroll injection... is an indication of a recent job loss.

Identify Anomalies

Feedzai ingests and utilizes session and behaviour type data, such as device and browsing patterns, and compares this data to customer profiles to identify anomalies.

Full Customer Journey Insight

Feedzai brings multiple external and internal data sources together and uses machine learning to derive greater insight into the customer journey.

Full Customer History Insight

Feedzai looks across the entire customer history and gleans information from seemingly unrelated events (e.g., previous logins from new devices) as potential indicators of fraudster reconnaissance.

Scam-specific Models

Prevention and detection models can be created independent of general fraud transaction models to identify scam behaviour specifically by creating scam-specific features that are indicative of fraud. This feature can be used alongside general transaction scoring to make better decisions.

Custom Rules

Rules can be tailored and grouped to include specific scam clauses that can be adapted as fraudsters change their patterns.

Specialized Alerts

White box explanations and rules triggered can be captured in Alerts along with specific indicators to help guide operations agents to have the right conversation with customers due to the complexity of scam fraud.

Routing to Specific Agents

If required, certain alerts can also be routed to specific agent groups via role and queue management to make sure those best trained are able to manage these alerts. In other cases, different queue parameters are required such as how quickly to respond to an alert.

Fraud Typology

Our dashboards and reporting can be separated by fraud typology to enable tracking of this MO in terms of detection and alert management.

Operational Execution Considerations

As noted earlier, detection of scams can be challenging for fraud operations analysts. There are a number of factors financial institutions should consider when creating or reviewing policy and procedure on transactions.

Operational Cheat Sheet / Red Flags Checklist

- ☐ **Does the transaction make sense for the customer demographic?**
  - Does the transaction **make sense** for the customer's age?
  - Is the transaction going to a **high-risk destination** (e.g., foreign currency or foreign IBAN).
- ☐ **Has the customer ever had a transaction like in the past?**
- ☐ **Does the transaction meet policy threshold for a must-call procedure?**
- ☐ **Does the transaction request fall outside the norm?**
  - **Odd contact** from family member (e.g., grandson calling claiming to be in jail)?
  - **BEC: Odd payment request**, or request from existing vendor for a change in payment instruction?
  - **Suspect transaction** (e.g.,1st time beneficiary and odd payment amount)?
  - **Repeated tractions** to unassociated beneficiary?
  - **Payment request** for money orders?

As a best practice, fraud operations calls should be recorded from a legal and liability standpoint. It's common for customers to validate the activity and insist the transaction be processed, only to later come back stating the transaction was indeed fraudulent as a result of the scam. Customers in certain situations will threaten legal action against the FI claiming negligence with approving the transaction. Call recordings will protect FIs against such allegations.

Finally, procedures and call scriptings should be reviewed and approved by line of business, business controls, compliance, legal, and HR teams to ensure they are enforceable and if necessary corrective action plans should be executed against them.

feedzai

One Platform to Manage Financial Crime

Build Your Business. We'll Protect it.

Every day, Feedzai's enterprise risk management platform scores trillions of dollars of transactions to protect the world's largest companies. Architected to be fully AI-enabled to stay ahead of emerging financial crime and money laundering patterns, Feedzai mitigates even the most deceptive criminals so that merchants, issuers, and acquirers can focus on growth.

feedzai.com

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