COMBATING FRAUD IN RETAIL AND TRAVEL:

Loyalty Platforms Latest Tactics

Sidney Dunn and Maciej Tyczynski
Director of Loyalty Consulting and Director of AI and Machine Learning
COMARCH LOYALTY
COMARCH LOYALTY

- 56,500 system users
- 8.1 billion processed loyalty transactions
- 90+ successfully implemented initiatives supported in 42 countries all over the world
- 290 million members of loyalty programs
- 1,200+ issuance & redemption program partners
- 620+ experts in 18 countries dedicated to marketing product development, implementation maintenance, sales, consulting program management and training
- 25 years on the market
- More than 17 years of experience & growth in customer loyalty management
- Our systems process more than 12 million transactions on a single system instance
## CLIENTS

<table>
<thead>
<tr>
<th>Oil &amp; Gas</th>
<th>Retail &amp; Consumer Goods</th>
<th>Travel</th>
<th>Airlines</th>
<th>Financial Services</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>bp</td>
<td>Auchan</td>
<td>ZURICH AIRPORT</td>
<td>jetBlue AIRWAY</td>
<td>CREDIT SUISSE</td>
<td>FMU</td>
</tr>
<tr>
<td>ExxonMobil</td>
<td>METRO GROUP</td>
<td>Heathrow</td>
<td>IAG</td>
<td>Jack Henry ERGONOMIC</td>
<td>aramex</td>
</tr>
<tr>
<td>OMV</td>
<td>Carrefour</td>
<td>Enterprise</td>
<td>Azul</td>
<td>Fosun</td>
<td>VinGroup</td>
</tr>
<tr>
<td>MAPCO</td>
<td>MediaMarktSaturn</td>
<td>Circuiit</td>
<td>SAS</td>
<td>Fosun</td>
<td>Netcetera</td>
</tr>
<tr>
<td>EG</td>
<td>True Value</td>
<td>DUBAIRPORTS</td>
<td>Norwegian</td>
<td>PRUDENTIAL</td>
<td>Tabcort</td>
</tr>
<tr>
<td></td>
<td>HBC</td>
<td></td>
<td></td>
<td></td>
<td>true</td>
</tr>
</tbody>
</table>

*COMARCH*
State of security
LIKELIHOOD OF CYBERATTACK IN 2019

How likely is it that your enterprise will experience a cyberattack next year?

- Very Likely: 34%
- Likely: 26%
- Somewhat Likely: 19%
- Neither Likely nor Unlikely: 7%
- Somewhat Unlikely: 2%
- Unlikely: 3%
- Very Unlikely: 2%
- Prefer Not to Say: 7%
"Collection #1": Over 770 million email addresses and 21 million unique passwords. A month later, additional 620 million accounts from 16 hacked websites. A total of 8.5 billion accounts leaked to date.

The group, called Fxmsp, claimed to breach the networks of McAfee, Symantec and Trend Micro, and steal 30 terabytes of data that they are offering for sale.

Highly sensitive personal data of over 100 German politicians, celebrities and journalists, including German Chancellor Angela Merkel, was leaked probably from their mobiles.

Airbus, the world’s second-largest manufacturers of commercial airplanes, was subject to a data breach exposing personal data of some of its employees.

More than 0.5 billion records of Facebook’s users were exposed by a third party on unprotected Amazon cloud servers.

Indian state-owned LPG Gas Company had online personal and sensitive data belonging to 7 million customers and distributors leaked following vulnerabilities in their iOS applications.

A misconfigured Elasticsearch DB on the Tommy Hilfiger Japan website led to the exposure of hundreds of thousands of customers’ personal information; full names, addresses, phone numbers, email addresses, date of birth, and transaction information.
FRAUDS IN LOYALTY PROJECTS WE SEE

Main types of loyalty frauds we see

Account Takeovers

Internal / Partner Fraud

Rule abuse
Account Takeovers

In loyalty context
**ATO IS A BUSINESS**

<table>
<thead>
<tr>
<th><strong>ACCOUNTS</strong></th>
<th><strong>IDENTITIES</strong></th>
<th><strong>MALWARE &amp; SERVICES</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online retailer gift cards</strong></td>
<td><strong>Stolen or fake identity</strong></td>
<td><strong>Office macro downloader generator</strong></td>
</tr>
<tr>
<td>15-50% of value</td>
<td>$0.10–150</td>
<td>$5–10</td>
</tr>
<tr>
<td><strong>Online banking accounts</strong></td>
<td><strong>Medical notes and prescriptions</strong></td>
<td><strong>Common banking Trojans toolkit with support</strong></td>
</tr>
<tr>
<td>0.5%–10% of value</td>
<td>$15–20</td>
<td>$10–1500</td>
</tr>
<tr>
<td><strong>Cloud service account</strong></td>
<td><strong>Mobile phone online account</strong></td>
<td><strong>Spyware</strong></td>
</tr>
<tr>
<td>$5–10</td>
<td>$15–25</td>
<td>$3–50</td>
</tr>
<tr>
<td><strong>Hacked email accounts (2,500)</strong></td>
<td><strong>ID/passport scans or templates</strong></td>
<td><strong>Money laundering service (into cash or</strong></td>
</tr>
<tr>
<td>$1–15</td>
<td>$1–35</td>
<td><strong>cryptocurrencies)</strong></td>
</tr>
<tr>
<td><strong>Retail shopping account</strong></td>
<td><strong>Full ID packages (name, address, phone, SSN,</strong></td>
<td><strong>Cash out service (bank account, ATM card,</strong></td>
</tr>
<tr>
<td>$0.50–99</td>
<td><strong>email, bank account, etc.)</strong></td>
<td><strong>and fake ID)</strong></td>
</tr>
<tr>
<td><strong>MONEY TRANSFER SERVICES &amp; CREDIT CARDS</strong></td>
<td><strong>Fake ID, driver license, passport, etc</strong></td>
<td><strong>Hacker for hire</strong></td>
</tr>
<tr>
<td><strong>Cash redirector service for bank accounts</strong></td>
<td>$25–5,000</td>
<td>$100+</td>
</tr>
<tr>
<td>1.15%–15% of value</td>
<td></td>
<td><strong>Custom phishing page service</strong></td>
</tr>
<tr>
<td><strong>Cash redirector service for online payment system</strong></td>
<td></td>
<td>$3–12</td>
</tr>
<tr>
<td>1–5% of value</td>
<td></td>
<td><strong>DDoS service, short duration &lt;1 hour</strong></td>
</tr>
<tr>
<td><strong>Pay $100 in Bitcoin and get a money transfer of $1000</strong></td>
<td></td>
<td>$5–20</td>
</tr>
<tr>
<td>$100</td>
<td></td>
<td><strong>Symantec ISTR24</strong></td>
</tr>
<tr>
<td><strong>Cash redirector service</strong></td>
<td></td>
<td><strong>Online retailer gift cards</strong></td>
</tr>
<tr>
<td>5–20% of value</td>
<td></td>
<td><strong>Online banking accounts</strong></td>
</tr>
<tr>
<td><strong>Single credit card</strong></td>
<td></td>
<td><strong>Cloud service account</strong></td>
</tr>
<tr>
<td>$0.50–20</td>
<td></td>
<td>$5–10</td>
</tr>
<tr>
<td><strong>Single credit card with full details (fullz)</strong></td>
<td></td>
<td><strong>Hacked email accounts (2,500)</strong></td>
</tr>
<tr>
<td>$1.45</td>
<td></td>
<td>$1–15</td>
</tr>
</tbody>
</table>

Source: Symantec ISTR24
IDENTITY THEFT, PHISHING

- Identity and credentials database leak can cost you much more than you expect.
- “GDPR” data penalties
  - British Airways: fined proposed: $240M (July 2019) “Poor security arrangements”
  - Marriott International Inc: fined proposed $128M (July 2019)
  - Facebook fined $650K (Oct 2018)
  - Equifax fined $650K (Sept 2018)
  - Chicago Broker Fined $1.5M for “Inadequate Cybersecurity”

- If you rely strictly on password based authentication, you’re an easy target for compromised credentials attack.

- Remedy: Strong customer authentication, Fraud detection, Penetration Tests, Procedures, Audits
PRESENTED EXAMPLES ARE A MIX OF EXAMPLES FROM BOTH PROJECTS USING COMARCH LOYALTY MANAGEMENT PLATFORM AND OTHER UNRELATED

COMPANY NAMES ARE OMITTED ON PURPOSE

SOME OF THE FIGURES AND STATS ARE Rounded

SOME OF THE DESCRIBED FRAUD CASES DIFFER FROM THE REAL SITUATION A LITTLE BIT FOR THE CONFIDENTIALITY PURPOSES, HOWEVER, THEY CARRY THE SAME MESSAGE
Example 1

**Industry**
Hospitality, Global

**What went wrong?**
Insufficient data security, infrastructure breach

**Background**
Compromised log-in credentials of a subset of loyalty members

**Detection method**
Darknet monitoring

**Fraud scenario**
Personal data were monetized as well free night vouchers redemptions were redeemed. In most of the cases – vouchers were sold on auctions and redeemed before member recognized missing points

**Loss**
Undisclosed
<table>
<thead>
<tr>
<th>Industry</th>
<th>What went wrong?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuel Retail, Europe</td>
<td>Fortunately it was detected and mitigated early, but some methods (like CAPTCHA) failed to prevent fraudsters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Background</th>
<th>Detection method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huge multinational loyalty scheme with 10s of millions of members acr</td>
<td>Infrastructure monitoring, IP address checks and blacklisting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fraud scenario</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stolen credentials used across multiple implementations. Using automated mechanisms and Upwork subcontractors To overcome CAPTCHA.</td>
<td>Couple of thousands euros</td>
</tr>
</tbody>
</table>
Internal / Partner Fraud

In loyalty context
Example 1

Industry
Retail, Europe

What went wrong?
Privilege abuse, insufficient security procedures in place

Background
Enrollment bonus for new accounts

Detection method
Reporting, fraud rule engine

Fraud scenario
Outsourced Contact Centre agents created new accounts using fake data, then merged multiple accounts and redeemed bonus points for discount vouchers

Loss
Undisclosed
<table>
<thead>
<tr>
<th><strong>Example 2</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Industry</strong></td>
</tr>
<tr>
<td>Fuel Retail, North America</td>
</tr>
<tr>
<td><strong>Background</strong></td>
</tr>
<tr>
<td>Over 10 different Point of Sales software used across stations.</td>
</tr>
<tr>
<td>Fraud rule that blocks accounts with more than 5 daily transactions.</td>
</tr>
<tr>
<td><strong>Fraud scenario</strong></td>
</tr>
<tr>
<td>Cashiers realized car wash sales are processed as a different transaction type than a regular sale.</td>
</tr>
<tr>
<td>Started swiping own cards whenever a customer was using car wash service and was not enrolled to loyalty</td>
</tr>
</tbody>
</table>
Example 3

**Industry**
Luxury retail, Europe

**What went wrong?**
System configuration, POS integrations

**Background**
Employee has been found guilty of fraud and theft after she accumulated **280,000 pounds** worth of loyalty card points from customers who failed to redeem them.

**Fraud scenario**
Employee was able to take advantage of point-of-sale hardware, scanning her own card instead of those belonging to paying customers.

**Detection method**
Semi-accident: Program owners noticed a large loyalty point balance under a variation of one customer-facing employee’s name. This was going on for 3 years before detected.

**Loss**
Unknown
Rule Abuse

In loyalty context
Industry
Oil & Gas, Europe

What went wrong?
A little too much trust in members

Background
It was possible to retro claim points for sale transactions as long as member provided time, location & value of transaction within 7 days after it happened.

Detection method
Reporting, security testing

Fraud scenario
People waiting at stations, checking the value of transaction at the pump and retro claiming transactions of other customers

Loss
Couple of thousands euros
Example 2

Industry
Travel, USA

What went wrong?
Typical case of rule loophole
Retailer failed to restrict serving size. The consumer purchased $0.25 individual-sized pudding cups and attained $25K worth of airline miles

Background
The frozen food company offered consumers the chance to earn 1000 airline miles for every 10 product barcodes submitted

Detection method
Unknown. Side note - now famously known as the Pudding Guy, he has his own Wikipedia page and YouTube video proudly explaining his exploit

Fraud scenario
2 million Airline Miles (valued at $25K) earned by buying 12,000 pudding cups as part of a promotion.

Loss
Couple of thousands USD
<table>
<thead>
<tr>
<th><strong>Example 3</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Industry</strong></td>
</tr>
<tr>
<td>Travel, USA</td>
</tr>
<tr>
<td><strong>What went wrong?</strong></td>
</tr>
<tr>
<td>Typical case of rule loophole related to point transfers &amp; conversions.</td>
</tr>
<tr>
<td><strong>Background</strong></td>
</tr>
<tr>
<td>Coalition travel loyalty program with a possibility to convert points accrued with one airline to another</td>
</tr>
<tr>
<td><strong>Detection method</strong></td>
</tr>
<tr>
<td>Unknown.</td>
</tr>
<tr>
<td><strong>Fraud scenario</strong></td>
</tr>
<tr>
<td>$60K first class suite for a round the world trip on Airline A issued to a travel blogger who knew how to convert his Airline B miles for one long trip with multiple layovers</td>
</tr>
<tr>
<td><strong>Loss</strong></td>
</tr>
<tr>
<td>~$60K</td>
</tr>
</tbody>
</table>
Leveraging Loyalty Platforms to Combat Fraud
FRAUD TRANSACTION PROCESSING IN CLM

Create transaction
CLM receives transaction

Business rules
Transaction is processed with the Business Rules engine

Transaction results
Change transaction status
Change account status
Change Customer status
Change user status

CLM
FRAUD RULE DEFINITION – SOURCE EVENT

**Transaction type**
- Transaction types which are monitored for a fraud activity

**Transaction channel**
- Channel for source event. More than one channel can be selected

**Condition formula**
- Source event triggering condition

Examples:
- Number of requested retro claims per day exceeds a given threshold
- Amount of points from a single accrual transaction exceeds the given limit
1. Counter that calculates number of redemptions made per day per member

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max value (counter limit)</td>
<td>999</td>
</tr>
<tr>
<td>Accumulation level</td>
<td>Account</td>
</tr>
<tr>
<td>Accumulation period</td>
<td>1 Day</td>
</tr>
<tr>
<td>Recognition qualifying</td>
<td>Never</td>
</tr>
<tr>
<td>Reverse type</td>
<td>max number of redemptions per day per card</td>
</tr>
</tbody>
</table>

2. Account is blocked once customer makes more than 3 redemptions a day.

- **Transaction**
  - `account.CounterValue('cnt_red') > 3`

- **Transaction result**
  - 33

- **Error return code**
  - Message: Redemption limit exceeded

- **Block account**
  - Block customer
  - Block user
FRAUD ACTIONS

Do not store transaction
- Cancel transaction, do not store its result and return an error code defined with the Business rule

Rejected
- Store transaction with status ‘Rejected’ without any results of transaction processing, e.g. points will not be accrued on Customer’s account

Booked
- Store transaction with original status and result but mark it as suspicious for further investigation

Booked break rules processing
- Store with original status and result but marked as suspicious for further investigation and break processing of other business rules
FRAUD ACTIONS – ADDITIONAL OPTIONS

**Block Account**
- Changes customer account's status to 'Blocked'
- Only for 'Booked' and 'Rejected' transaction results

**Block Customer**
- Changes customer's status to 'Blocked'
- Only for 'Booked' and 'Rejected' transaction results

**Block user**
- Changes CC agent's status to 'Blocked'
- CC agent is automatically logged out from the CC application

**Create CC case**
- Automatically created to inform a CC agent that a fraud was detected
- Only for 'Booked' and 'Rejected' transaction results
FRAUD TRACKING

Call center application

- **Case activities** to instantly track suspicious (status 'Booked') or rejected ('Rejected') transactions
- Case activity is be assigned to a default CC agent as defined in the case configuration
- Other agents may also be assigned to the case (they will receive e-mail notification)

- **E-mail notifications** sent to CC agents
- Notification is sent to agents assigned to the case type

Reports

- Fraud detection reports can be generated in the Comarch BI
FRAUD MANAGEMENT – PREVENTION POSSIBILITIES IN CLM

**Automatic**
- Account blockage when limit is exceeded
- Transactions rejection when limit is exceeded
- Redemption transaction rejection limit is exceeded
- Contact Center case creation
- Call Center user blockage when limit of manual operation is exceeded
- Generate daily report with all records rejected by the anti-fraud rule and accounts blocked

**Manual**
- Monitoring based on reports
- Verification of all criteria of potential frauds
- Particular account’s transactions verification (when one of criteria met)
- Compare number of transactions made by cashiers in the shop (if one has many more than others)
- Verify accounts with highest points balance
- Manual account blockage (suspension) for verification reasons

Solution exists in CLM
Requires BI Reporting
# FRAUD MANAGEMENT – MOST FREQUENT ISSUES AND SOLUTIONS, BASED ON OUR EXPERIENCE

<table>
<thead>
<tr>
<th>Suspicious behavior</th>
<th>Solution</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>One card is scanned many times by one cashier in a day / week</td>
<td>Limit number of purchase transactions per customer per day/week, potentially per shop</td>
<td>Reject transaction that exceeded a limit and block account</td>
</tr>
<tr>
<td>Very high purchase transaction value (way above average)</td>
<td>Limit on single transaction value</td>
<td>Reject transaction that exceeded a limit and block account</td>
</tr>
<tr>
<td>Different method of payments visible on one card</td>
<td>Report showing a transactions breakdown by methods of payment per account</td>
<td>List and verify accounts with mixed method of payments</td>
</tr>
<tr>
<td>Many redemptions on one card</td>
<td>Limit on number of redemptions per customer per day. Potentially set limit per store</td>
<td>Reject transaction that exceeded a limit and block account</td>
</tr>
<tr>
<td>Very high redemption value (huge number of points redeemed)</td>
<td>Limit on single redemption value</td>
<td>Reject transaction that exceeded a limit and block account</td>
</tr>
<tr>
<td>High value product returns</td>
<td>Limit on number of returns per member</td>
<td>Reject return that exceeded a limit and block account</td>
</tr>
<tr>
<td>Transactions in two shops being far away from each other made in one day</td>
<td>Limit on transactions made in two different stores, per day, per member</td>
<td>Block account</td>
</tr>
</tbody>
</table>
The Next Frontier
How Loyalty Platforms are leveraging AI to get ahead of the fraudsters
Loyalty Fraud – traditional countermeasures

<table>
<thead>
<tr>
<th>Fraud countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal data</strong></td>
</tr>
<tr>
<td>- De-duplication</td>
</tr>
<tr>
<td>- Blacklisting</td>
</tr>
<tr>
<td>- Address checks</td>
</tr>
<tr>
<td>- Email / phone verification</td>
</tr>
<tr>
<td><strong>Program configuration</strong></td>
</tr>
<tr>
<td>- Delayed point posting</td>
</tr>
<tr>
<td>- Address / ID accounts limitations</td>
</tr>
<tr>
<td>- Key processes handling verification</td>
</tr>
<tr>
<td>- Fraud rules / limits in a number of operations</td>
</tr>
<tr>
<td><strong>End-point security</strong></td>
</tr>
<tr>
<td>- 2FA</td>
</tr>
<tr>
<td>- OTP</td>
</tr>
<tr>
<td>- Browser / bot prevention</td>
</tr>
<tr>
<td>- Security audits</td>
</tr>
<tr>
<td>- Password policies</td>
</tr>
<tr>
<td><strong>User management</strong></td>
</tr>
<tr>
<td>- Minimum required access</td>
</tr>
<tr>
<td>- Additional approval</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
</tr>
<tr>
<td>- Program statistics</td>
</tr>
<tr>
<td>- KPIs</td>
</tr>
</tbody>
</table>
Assumptions are great, until they are not.

M. Tyczynski, 2019
LOYALTY FRAUD CASES

Hackers Have A New Target: Your Frequent Flyer Miles

IT manager jailed for awarding himself 14 million Nectar points

How much are stolen frequent flyer miles worth on the dark web?

At least 10 major loyalty card schemes compromised in industry-wide scam

Russian cyber criminals stealing British people's reward points and airmiles to go on luxury holidays

Radisson Suffers Global Loyalty Program Data Breach

The true impact of loyalty card fraud

Police officer fiddled 75,000 points on Tesco loyalty card

COMARCH
Machine Learning for Loyalty Fraud

- Fraud Rules
- End-point security
- Reporting
- Monitoring & KPIs
- Machine Learning
AI for loyalty fraud detection
AI for loyalty fraud detection

- **Spend** activity
- Point **balance change**
- Time between interactions
- **Locations** of purchases
- Average **interaction values**
- Earn to Burn **ratios**
- Clusters of members with **similar activity**

- Predictions of how a „typical member“ behave
Example

Found:
- Accounts with **odd earn to burn ratios**
- Series of **repeated accrual or redemption transactions**
- Redemptions way bigger than the average
- Series of transactions happening in a very small timeframe
- Big manual **point corrections**
- Repeated **transaction reversals**
- Accounts with **quick balance gains**
LOYALTY FRAUD – REINFORCEMENT LEARNING

Assets
Money
Coupons

... Rest API ... CLM

Business Rules
Constraints
Products
Points
Rewards

...
Summary:

- Fraudsters are getting smarter
- Information spreads much quicker than ever before
- AI/ML can be a game changer
- Historical data is key
- Define what is normal and what is a fraud from many perspectives
- Train, Validate, Iterate
- Implement in a consistent manner
- Mind the false positives

Source: https://xkcd.com/1317/