Identity War Games: A Learning Lab on Account Opening Fraud

Uri Rivner
Chief Cyber Officer
BioCatch
LinkedIn: Uri Rivner

Erin Englund
Senior Threat Analyst
BioCatch
LinkedIn: Erin Englund
** [GlobalData] - Highest quality information provider. Any state and gender available. **

** Update: Husband and Wife profiles available. Product details: High Quality FICO Profile Format: First name Last name SSN DOB Civil Status Address City ...**

Sold by **globaldata** - 966 sold since **Dec 12, 2015**

<table>
<thead>
<tr>
<th>Features</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product class</td>
<td>Digital goods</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Ends in</td>
<td>Never</td>
</tr>
<tr>
<td>Origin country</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Ships to</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Payment</td>
<td>Escrow</td>
</tr>
</tbody>
</table>

**Extra requirements (DOB + State + Background Report + 650 FICO) - 1 days - USD +29.50 / item**

**Extra requirements (DOB + State + Background Report + 720 FICO) - 1 days - USD +49.50 / item**

**Extra requirements (DOB + State + Background Report + 780 FICO) - 1 days - USD +69.50 / item**

**Extra requirements (DOB + City + State + Background Report + 750-820 FICO) - 1 days - USD +100.00 / item**

**Extra Requirements (Husband & Wife + DOB + State + BACKGROUND REPORTS + 720 FICO) - 1 days - USD +86.50 / item**

Source: Palo Alto Networks
AO Fraud growing fast

U.S. DDA Application Fraud, 2015 to e2020 (US$ Millions)

Source: AITE

- Credit card
- DDA

<table>
<thead>
<tr>
<th>Year</th>
<th>Credit card</th>
<th>DDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>$466</td>
<td>$1,169</td>
</tr>
<tr>
<td>2017</td>
<td>$541</td>
<td>$1,368</td>
</tr>
<tr>
<td>2018</td>
<td>$600</td>
<td>$1,614</td>
</tr>
<tr>
<td>e2019</td>
<td>$648</td>
<td>$1,888</td>
</tr>
<tr>
<td>e2020</td>
<td>$694</td>
<td>$2,096</td>
</tr>
</tbody>
</table>
Identity Under Attack

<table>
<thead>
<tr>
<th>Data Breach Victims</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN</td>
<td>35%</td>
</tr>
<tr>
<td>Credit card number</td>
<td>30%</td>
</tr>
<tr>
<td>Debit card number</td>
<td>16%</td>
</tr>
<tr>
<td>Online banking credentials</td>
<td>8%</td>
</tr>
<tr>
<td>Checking account number</td>
<td>7%</td>
</tr>
<tr>
<td>Driver’s license number</td>
<td>6%</td>
</tr>
<tr>
<td>Medical records or health insurance info</td>
<td>5%</td>
</tr>
<tr>
<td>Debit card PIN</td>
<td>3%</td>
</tr>
<tr>
<td>Credit card ATM PIN</td>
<td>3%</td>
</tr>
<tr>
<td>Child’s SSN</td>
<td>2%</td>
</tr>
<tr>
<td>School records</td>
<td>1%</td>
</tr>
<tr>
<td>Military ID</td>
<td>0%</td>
</tr>
</tbody>
</table>

Source: Javelin Strategy & Research, 2018

Areas of Greatest Concern Regarding Fraud

- **27%** Payment fraud
- **23%** Account takeover
- **15%** Call center fraud
- **3%** Other
- **32%** New account synthetic or stolen identity fraud

Base: All respondents’ risk and security management, n = 297
Q: In your organization, which area of fraud prevention is currently of the greatest concern?
ID: 325713

© 2018 Gartner, Inc.
Investment in next-gen lines of defense rising

Q. Do you plan to add or change DDA application risk assessment vendors in the next 1 to 2 years?  
(Among respondents responsible for new customer onboarding process for DDA)

<table>
<thead>
<tr>
<th>2015 (n=56)</th>
<th>2018 (n=27)</th>
</tr>
</thead>
<tbody>
<tr>
<td>68%</td>
<td>48%</td>
</tr>
<tr>
<td>18%</td>
<td>15%</td>
</tr>
<tr>
<td>9%</td>
<td>33%</td>
</tr>
<tr>
<td>5%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Yes, we plan to replace one or more current vendors with a new vendor
- Yes, we plan to add additional vendors
- We plan to decrease or consolidate vendors
- No changes planned in the next 1 to 2 years

Source: Aite Group
Welcome to the Battle of Identity War Games

• Alright... It’s a BIG problem!
• And we’re all here to fight it!!!
• Principles of our War Games:
  • You are the fraud team
  • You’ll need to make quick decisions about identity
  • You do have access to a LOT of data
  • Cases are all REAL
  • PII presented is NOT real
  • Who are these kids in the photo?
You’ll need to leverage multiple signals to succeed

What You Know (User Data)
- KYC Data
- Residences & Licenses
- Credit History

What you Have (User Resources)
- Device
- IP Location
- Phone

What You Do (Digital Footprint)
- Social Media Reputation
- Email Reputation
- Open Source Analysis

What You Are (User Behavior)
- Familiarity with Data
- Familiarity with Process
- High User Expertise
Just to get us started

Individual votes
What’s your verdict? Good or Bad?
Top 5 Credit Card Issuer

First name pasted 3 sec into session

Confirmed as fraud
What’s your verdict? Good or Bad?
Top 5 Credit Card Issuer

<table>
<thead>
<tr>
<th>Customer Session ID</th>
<th>MUID</th>
<th>Date &amp; Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>82f45ee9bab4217865cb4db90a46112</td>
<td>4973F8685-0C1-...</td>
<td>15.06.2017</td>
<td>09:10</td>
</tr>
<tr>
<td>1d204922d304c67aaa1e46e63ef021</td>
<td>4973F8685-0C1-...</td>
<td>15.06.2017</td>
<td>07:55</td>
</tr>
</tbody>
</table>

KYC Checks – 100% match

User clicked on F12 to open the Developer Tools

Confirmed as fraud

High ground speed (UK to Ukraine in 1:15 hours)
A Training Scenario

Practice Round!
Rules of Engagement

- Each table is a fraud team
  Your objective is to reach the quickest *correct* decision

- An initial summary is provided followed by data points, one by one

- Discuss the details of the case within your team

- Following each data point, I will ask for your team’s decision

- Each team member can have one of the following votes:
  - FRAUD! 👎
  - GENUINE! 😊
  - Inconclusive... We want more DATA! 🤔👍
Before we start

- It’s time for each member of a fraud team to introduce themselves to their colleagues around the table.
- Tell the folks who you are, your current role, and what’s your background or interest in online fraud detection.
- Is everyone ready?
Training Scenario
Based on a true story, with modifications to fit the Battle of Identity War Games

You’re the fraud team of a large credit card issuer. There’s a new application under review:

- All the KYC checks passed: Name, DOB, SSN
- Main risk factor: email provided is less than 10 days old
- This triggered a step-up authentication: User asked to photo their Driver’s License – which passed

Account Application Details
- Name: Alan Bishop
- Date of Birth: May 21, 1982 (37 years old)
- Phone: 627-844-6235
- Address: 511 Spruce Ave, Cambridge, 01743
- Email: abishop3454@gmail.com
Data Point #1

Address provided is not a valid address

- 511 Spruce Ave does not exist
- But 51 Spruce Ave is valid address, record shows user has been there for 7 years. Typo?

Account Application Details
- Name: Alan Bishop
- Date of Birth: May 21, 1982 (37 years old)
- Phone: 627-844-6235
- Address: 51 Spruce Ave, Cambridge, 01743
- Email: abishop3454@gmail.com
Social Media Footprint for Alan

- LinkedIn: Yes, 60 connections, works in Boston area
- Facebook: Yes, 97 friends, lives in Cambridge
- Email connected to both accounts: Alan.Bishop@gmail.com
- abishop3454@gmail.com is a few days old

Account Application Details
- Name: Alan Bishop
- Date of Birth: May 21, 1982 (37 years old)
- Phone: 627-844-6235
- Address: 511 Spruce Ave, Cambridge, 01743
- Email: abishop3454@gmail.com
Data Point #3

Phone is a prepaid mobile

- The phone number doesn’t match the specific address
- It’s not on record for this person despite being registered for 6 years

Account Application Details
- Name: Alan Bishop
- Date of Birth: May 21, 1982 (37 years old)
- Phone: 627-844-6235
- Address: 511 Spruce Ave, Cambridge, 01743
- Email: abishop3454@gmail.com
What’s your verdict? Good or Bad?

Confirmed as Fraud

• Fraudster found Alan’s driver license on the steps of 51 Spruce Ave in Cambridge and used it to apply for a credit card
Enough Chit Chat!

- Time for the REAL ACTION
- We have 3 Identity War Games scenarios
- In each scenario, you can ask for up to 5 data points
- Your goal is to get to the quickest *correct* decision for each scenario
- READY?
War Games Scenario 1

Call the Dead Guy
A big hotel chain issues a credit card

There is a specific application that the model recommends **declining**:

- Model score is **96** out of **100**
- Main risk factor: **SSN is suspicious**
- This triggered a call to the user’s land line on record. Result: **no answer**

**Credit Card Application Details**
- **Name:** Thomas Green
- **Date of Birth:** May 26, 1996 (22 years old)
- **SSN:** 550-36-9100
- **Phone:** 505-344-3294
- **Address:** 7213 Coulson Dr NE, Albuquerque NM 87109-5400
- **Email:** Thomas.T.Green80@gmail.com
Data Point #1

Device and Phone Reputation

- Device ID does not match criminal activity
- IP spoofing / Virtual Machine not detected
- Provided phone first seen 2 years ago

Credit Card Application Details
Name: Thomas Green
Date of Birth: May 26, 1996 (22 years old)
SSN: 550-36-9100
Phone: 505-344-3294
Address: 7213 Coulson Dr NE, Albuquerque NM 87109-5400
Email: Thomas.T.Green80@gmail.com
Data Point #2

KYC: SSN Analysis

- Name on Record: Richard Gowdy
- Phone on Record: 520-768-8988 (inactive)
- Address on Record: 1601 N 9th Ave Tucson AZ
- Date of Birth: Apr 24, 1937
- Date of Death: Nov 12, 2008
Data Point #3

How familiar are you with the data?

- SSN typed continuously
- Looks like this is done from long-term memory rather than typing off a list

Credit Card Application Details
Name: Thomas Green
Date of Birth: May 26, 1996 (22 years old)
SSN: 550-36-9100
Phone: 505-344-3294
Address: 7213 Coulson Dr NE, Albuquerque NM 87109-5400
Email: Thomas.T.Green80@gmail.com
Data Point #4

How familiar are you with the Process?

- User required to submit hotel loyalty program number
- Time to provide hotel loyalty number: 58 seconds

Session timeline

58 sec to provide Hotel loyalty number

Credit Card Application Details
Name: Thomas Green
Date of Birth: May 26, 1996 (22 years old)
SSN: 550-36-9100
Phone: 505-344-3294
Address: 7213 Coulson Dr NE, Albuquerque NM 87109-5400
Email: Thomas.T.Green80@gmail.com
Data Point #5

Social Media Footprint

- Facebook: YES, 76 friends
- Instagram: YES, last action 3 days ago
- Email linked to these accounts: Thomas.T.Green80@gmail.com

Credit Card Application Details
Name: Thomas Green
Date of Birth: May 26, 1996 (22 years old)
SSN: 550-36-9100
Phone: 505-344-3294
Address: 7213 Coulson Dr NE, Albuquerque NM 87109-5400
Email: Thomas.T.Green80@gmail.com
What’s your verdict? Good or Bad?
Hotel Chain Credit Card

Confirmed as Genuine
• User mistyped his SSN
• Team contacted user – he now has a credit card

Quick Discussion:
• What’s the cost of a false decline?
Summary
Call the Dead Guy

- KYC controls look for many correlations and try matching many factors, but sometimes the data is biased, faulty, not up to date – or the user just makes a mistake.
- Using next-gen data sources that don’t actually use the data itself can provide a ‘second opinion’ that clears applications, leading to higher acquisition rates.
War Games Scenario 2

Defying the Laws of Physics
Scenario #2

Bob tried requesting a ride through a rideshare app, but was **blocked**

He emailed the Risk Team to try and understand what’s going on

**Block reasons:**
- A credit card belonging to Bob was used in a new account created by Maureen
- The app was downloaded in Hong Kong and used in Asia

Time is of the essence... the team needs to quickly investigate and decide:
- If this is fraud, Bob should immediately cancel his card and reset his password
- If this is genuine, the team should manually override the block and contact Bob

**Name:** Maureen Santiago  
**Date of Birth:** Jan 14, 1987 (31 years old)  
**Phone:** 310-081-0943  
**Address:** 294 Sloan Street, Beverly Hills, 90210  
**Email:** Maureen.Santiago87@gmail.com
Data Point #1

Location analysis on Bob’s account

- Bob requested rides in several locations in US, and some locations in Mexico and Europe
- His last 3 months of activity focused on trips in Silicon Valley and Los Angeles areas
Data Point #2

Uses of Bob’s Credit Card in the app

Rides requested (Bob)
- Feb 11: Los Angeles
- Feb 13: Los Angeles

Rides requested (Maureen)
- Feb 11: Hong Kong
- Feb 12: Bangkok
- Feb 14: Singapore
Data Point #3

Maureen’s Email Reputation Analysis

- Maureen’s email account is 8 years old
- Email was created in Manila, Philippines
Data Point #4

Social Media Footprint for Maureen: Basic

- Facebook: YES, 4,718 friends, Lives in Beverly Hills
- Instagram: YES, Last action 3 hours ago from Singapore
- Twitter: YES, Last action 1 day ago
- Email linked to these accounts: Maureen.Santiago87@gmail.com (same one as used to open the account in the share riding app)
Social Media Deep Dive

- Facebook: Maureen is a model born in the Philippines
- Instagram: Shows current photos from her Thailand location shooting
What’s your verdict? Good or Bad?

Confirmed as Legitimate

- Bob had given his credit card to Maureen, his girlfriend.
- She is a model and travels internationally.

Quick Discussion:

- Is social media analysis useful?
Summary
Defying the Laws of Physics

- Having multiple layers of visibility is key
- Social media analysis can provide negative and positive clues, but may be difficult to fully automate and easy to get into a rabbit hole if you’re not careful.
War Games Scenario 3

Save the Sea Turtles
Scenario #3

A bulk order of paper straws for the sum of $25,000 is flagged for review.

Flag reasons:
- Order value is higher than average from a first-time seen credit card, though the merchant typically sells in bulk to restaurants
- An international shipping address with expedited shipping was entered at check out

This is a pending order. The team needs to review and decide:
- If this is a good order from an international customer, then allow
- If this is fraud and should be declined before resulting in a chargeback
- If this is fraud, is the merchant a victim or in collusion with the buyer?
Data Point #1

Who is the merchant?

- The merchant is a paper straw supplier, EcoStraws, based in San Diego, CA
- The merchant accepts web orders or phone-in orders
- The majority of high-value transactions come from restaurants buying in bulk
- International shipping is available for web and bulk orders

<table>
<thead>
<tr>
<th>Product Type</th>
<th>Price Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assorted 100 Packs</td>
<td>$4.95 - $5.95</td>
<td>Jumbo Cocktail size (6x197mm - 0.24&quot;x7.75&quot;)</td>
</tr>
<tr>
<td>Unwrapped 250 Packs</td>
<td>$8.95</td>
<td>Jumbo Cocktail size (6x197mm - 0.24&quot;x7.75&quot;)</td>
</tr>
<tr>
<td>Wrapped 250 Packs</td>
<td>$9.95</td>
<td>Jumbo Cocktail size (6x197mm - 0.24&quot;x7.75&quot;)</td>
</tr>
<tr>
<td>Boba/Bubble Tea 200 Packs</td>
<td>$19.95 - $24.95</td>
<td>Colossal size (12x197mm - 0.47&quot;x7.75&quot;)               Diagonal Cut Tip</td>
</tr>
</tbody>
</table>
Data Point #2

What do we know about the transaction?

- 62 crates
- 740,000 straws
- $25,616 USD paid in full
- Top 10 US Bank corporate credit card
- Billing address for card is in US
Data Point #3

Shipping Address Analysis

- **$9,490 USD** for urgent 2-day shipping to Tuvalu
- Shipping address: 404 Ashley Street, Viaku, Tuvalu
- You’ve got a few min to do your own research...

Welcome to Tuvalu, population 11,000
Data Point #4

How was the payment method entered?

- Card number, CVV code and Zip code are all pasted using Ctrl-V
- Expiration date is typed
- Pasting zip code is very unusual – 0.12% of users paste the zip code
Data Point #5

A call to the merchant...

- After the payment went through, the buyer called the merchant to say the shipping cost is crazy
  - Requested to use their own preferred shipping company
  - Asked to wire the amount already paid for shipping ($9,490 USD) to that shipping company’s bank account
  - The shipper will pick up the shipment from the merchant’s warehouse

- Some research reveals the following about the buyer’s chosen shipping company:
  - Based in Los Angeles, CA
  - Website domain opened 3 months ago
  - Freight forwarder specializing in shipments from US to Asia-Pacific region

- This is a very urgent order! The shipping company is waiting on stand-by
What’s your verdict? Good or Bad?

Emergency Straw Shipment

**Confirmed as Fraud**
- User selected the most expensive shipping method & country possible
- User requested the merchant forward the shipping cost directly to their fraudulent shipper

Quick Discussion:
- What would be the impact of a $25K fraud chargeback for a small merchant?
What about the merchant – victim or collusion?

- The merchant is the manufacturer, wholesaler, and retail provider of paper straws operating since May 2018
  - Employs 40 people in San Diego, CA

- **Social Media Footprint:**
  - Facebook: YES 481 followers with a 5-star rating
  - Instagram: YES 776 followers
  - Twitter: YES 1,896 followers
  - Featured recently in Slate.com

- The Tuvalu order is an anomaly for this merchant – 99% of transactions ship to US addresses
What’s your verdict? Good or Bad?
Emergency Straw Shipment

Victim!
- The merchant is a small business with a small, but faithful & growing customer base... and no experience with fraud prevention
- A fraud chargeback of $25K could be a major set back for a small merchant

Quick Discussion:
- How do you enable your fraud operations team to review collusion and account linking?
• The bigger the transaction, the higher the risk, but also the higher the reward. This could have easily been a real case of a huge, unusual order

• Which is why just transactional data is insufficient. It takes many layers of analysis to make an informed decision
Summary and Q&A
What Have We Learned From Our War Games?

There are a variety of data sources to review:
- Resource Correlation (Email, Phone)
- Device and Location Reputation
- Social Media and Digital Footprint
- Behavioral Biometrics

Decisions are increasingly complex – but more insightful

It’s never a single incriminating fact – multiple data points need to be considered

And the most important thing:

When in doubt...
Call the Dead Guy!
Apply What You Have Learned Today

- **Next week you should:**
  - Identify data sources available within your organization to investigate fraud

- **In the first three months following this presentation you should:**
  - Conduct a deep dive review of missed fraud cases and false positives
  - Identify gaps in data, tools, and/or operational process
  - Establish areas where measurable improvements can be made
  - Celebrate your fraud team’s wins – where big losses were prevented

- **Within six months you should:**
  - Build a plan to close the gaps and set a realistic target that makes business sense
  - Set a regular cadence for revisiting your operational improvement plan and setting new targets (e.g. annually)
  - Build a fraud prevention case study to promote the work your fraud team is doing internally
Q&A

LinkedIn: Uri Rivner
LinkedIn: Erin Englund