

Third-Party Account Takeover Fraud in the Life Insurance Industry

The History, Schemes, Scams and Industry Response

Presented by: Russell Anderson, CFE - October 21, 2022

The Agenda

- First Some History
- It’s all About the Data
- The Schemes and Scams
- Meet The Fraudsters
- Industry Response
- The Opportunity
- Industry Collaboration



Account Takeover Fraud – History

Prior to ~2015 3rd Party ATO Fraud Practically Unheard of in the U.S. Insurance market





Digital transformation provides fraudsters greater anonymity and additional attack vectors



Cybercriminals have successfully accessed and made available virtually all of our personal data

Account Takeover Fraud – History



Prior to ~2015 3rd Party ATO Fraud Practically Unheard of in the U.S. Insurance market

- Trillions of Dollars in Insurance and Retirement Accounts
  - **$305k** Avg. Balance Targeted YTD 2022
  - **$70k** Avg. Fraudulent Withdrawal Requested YTD 2022
- Controls Not Designed to Prevent
  - Name, SSN, Date of Birth and Maybe an Address

Account Takeover Fraud – History

Digital transformation provides fraudsters greater anonymity and additional attack vectors



- Less Friction = Greater Customer Satisfaction & Fraud
  - Easy Online Access
  - Friendly Accommodating Customer Service Representative
  - Easy Account Access to Make Changes and Withdraw Funds

Account Takeover Fraud – History



Cybercriminals have successfully accessed and made available virtually all of our personal data

Assumption – Some Amount of All Our Data Has Been Exposed

yahoo! Over 3 Billion User Accounts exposed – Name, emails, Phone, DOB, Passwords, Security Questions (2013 – 2016)

EQUIFAX 163 Million (1/2 US Population) Names, SSN's, DOBs, Addresses and much more exposed (2017)

Capital One 100 Million Customer Bank Accounts, Names, Addresses, SSNs and Canadian SINs Stolen by an Employee (2019)

Microsoft 60,000 Companies email servers exposed and unknown amount of unknown data (2021)

T-Mobile 76 Million customer in 5 breaches between 2018 – 2021 exposed Names, Addresses, SSNs, Phone #'s, Drivers License #'s, DOBs and unknown amount of phone identifying data

Most Common Password in 2021 = qwerty, password, & 12345
65% Use the Same password

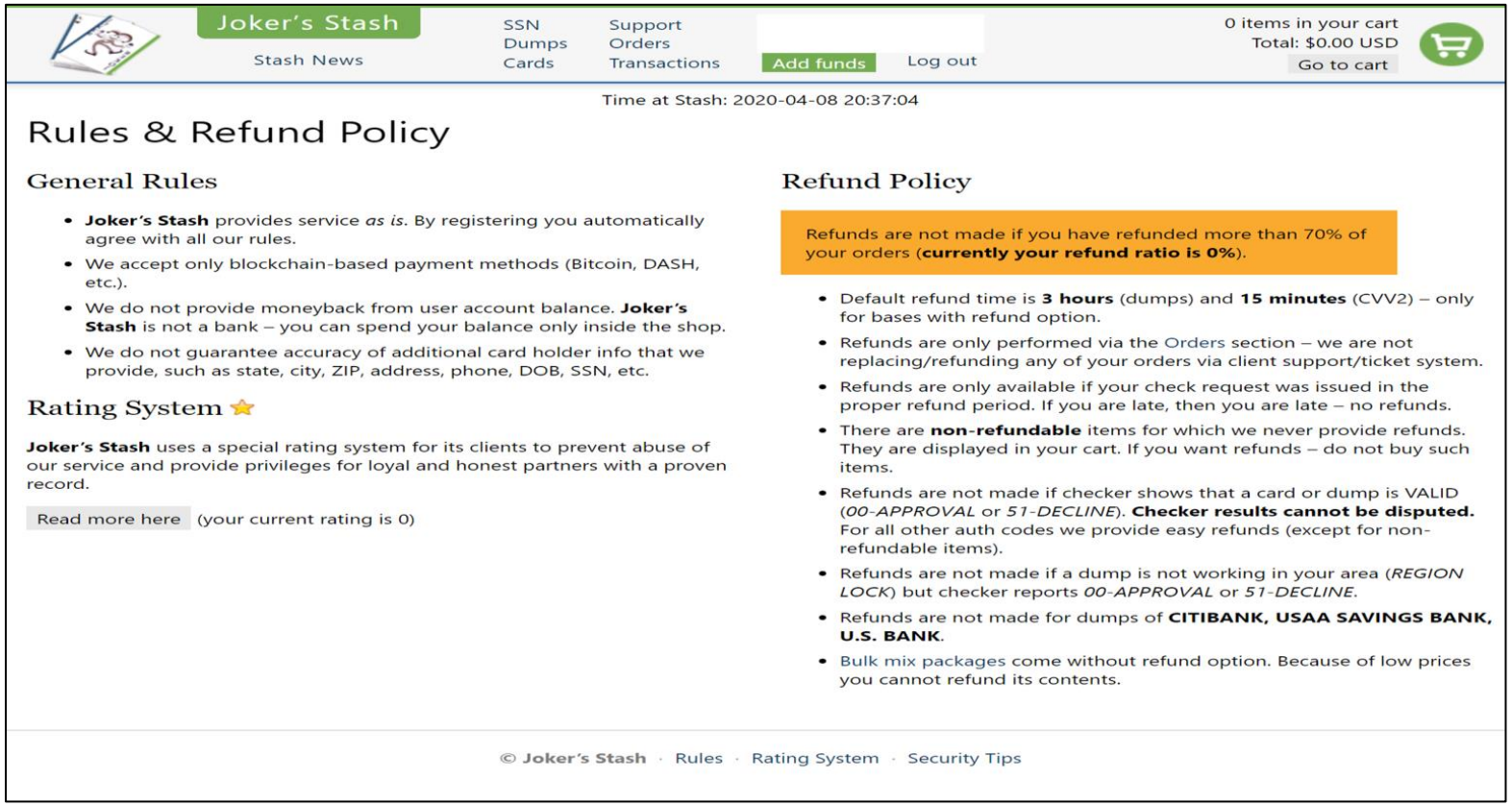
LIMRA LOMA

Account Takeover Fraud – It's All About The Data

Dark Web Market Places

- Very Legitimate Illegitimate Businesses
- They Have Rules
- Refund Policies
- Rating Systems

Jokers Stash



Joker's Stash

Stash News

SSN
Dumps
Cards

Support
Orders
Transactions

Add funds

Log out

0 items in your cart
Total: $0.00 USD
Go to cart

Time at Stash: 2020-04-08 20:37:04

Rules & Refund Policy

General Rules

- **Joker's Stash** provides service *as is*. By registering you automatically agree with all our rules.
- We accept only blockchain-based payment methods (Bitcoin, DASH, etc.).
- We do not provide moneyback from user account balance. **Joker's Stash** is not a bank – you can spend your balance only inside the shop.
- We do not guarantee accuracy of additional card holder info that we provide, such as state, city, ZIP, address, phone, DOB, SSN, etc.

Rating System

Joker's Stash uses a special rating system for its clients to prevent abuse of our service and provide privileges for loyal and honest partners with a proven record.

Read more here (your current rating is 0)

Refund Policy

Refunds are not made if you have refunded more than 70% of your orders (**currently your refund ratio is 0%**).

- Default refund time is **3 hours** (dumps) and **15 minutes** (CVV2) – only for bases with refund option.
- Refunds are only performed via the Orders section – we are not replacing/refunding any of your orders via client support/ticket system.
- Refunds are only available if your check request was issued in the proper refund period. If you are late, then you are late – no refunds.
- There are **non-refundable** items for which we never provide refunds. They are displayed in your cart. If you want refunds – do not buy such items.
- Refunds are not made if checker shows that a card or dump is VALID (*00-APPROVAL* or *51-DECLINE*). **Checker results cannot be disputed.** For all other auth codes we provide easy refunds (except for non-refundable items).
- Refunds are not made if a dump is not working in your area (*REGION LOCK*) but checker reports *00-APPROVAL* or *51-DECLINE*.
- Refunds are not made for dumps of **CITIBANK, USAA SAVINGS BANK, U.S. BANK**.
- Bulk mix packages come without refund option. Because of low prices you cannot refund its contents.

© Joker's Stash · Rules · Rating System · Security Tips

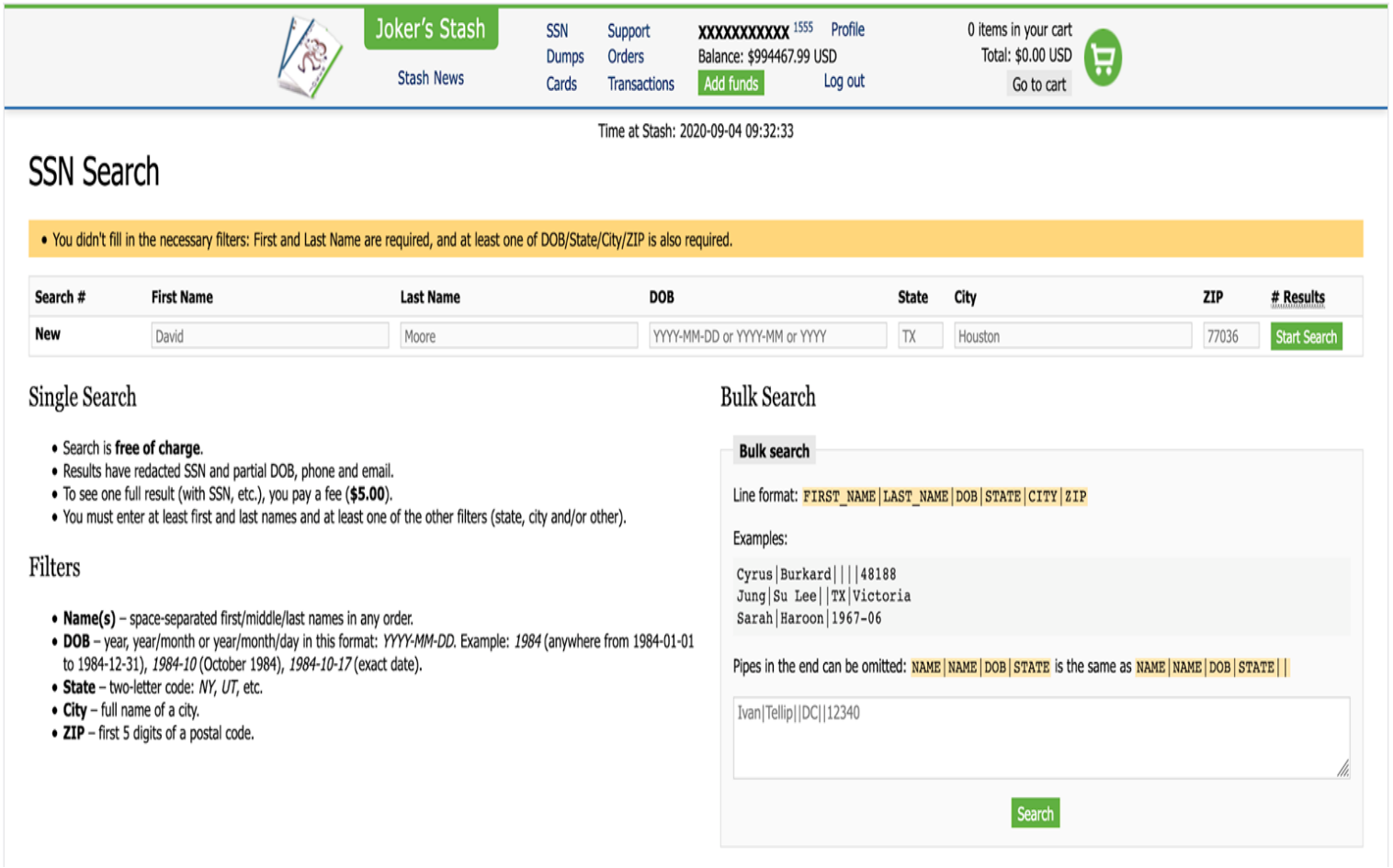
Account Takeover Fraud – It's All About The Data

Jokers Stash



No SSN – No Problem

You can buy it for $5



Account Takeover Fraud – It's All About The Data

2021-01-15

Finale



---- ENG ----

Joker goes on a well-deserved retirement. Joker's Stash is closing.
When we opened years ago, nobody knew us. Today we are one of the largest cards/dumps marketplace.
Unfortunately, or fortunately - nothing lasts forever. It's time for us to leave forever.
We will leave the Stash opened for 30 more days, until 2021-02-15, so all Stash users can spend accounts balances.
On 2021-02-15 we will wipe all our servers and backups and Joker will fade to dark, forever.
And mark my word: WE WILL NEVER EVER OPEN AGAIN! Do NOT trust possible future imposters!
After 2021-02-15 there will be no more Joker and no more Joker's Stash.
Dear partners of Stash - you can be sure, that before we leave forever, you will get all payouts, contact me you know how.

We are also want to wish all young and mature ones cyber-gangsters not to lose themselves in the pursuit of easy money.
Remember, that even all the money in the world will never make you happy and that all the most truly valuable things in this life are free.

Even Fraudsters Retire

Cybercrime Joker Retires With A Reported $2.1 Billion In Bitcoin

LIMRA LOMA

Account Takeover Fraud – It's All About The Data

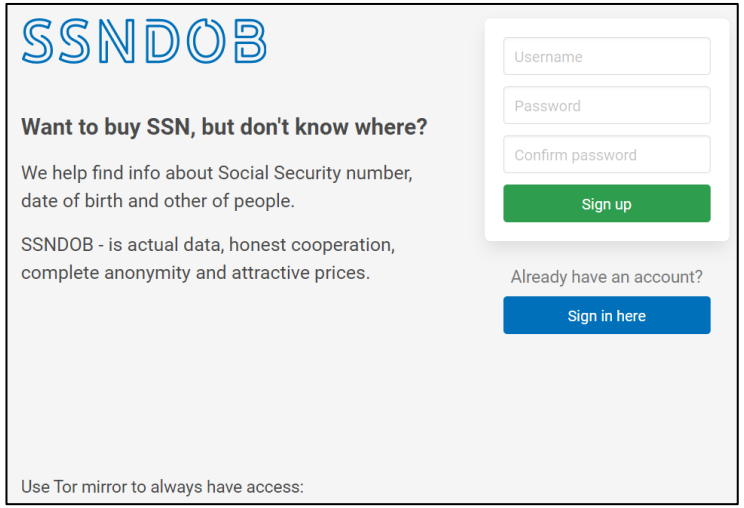
Sometimes The Good Guys Win

FOR IMMEDIATE RELEASE

Tuesday, June 7, 2022

SSNDOB Marketplace, A Series Of Websites That Listed More Than 20 Million Social Security Numbers For Sale, Seized And Dismantled In International Operation

Tampa, Florida – United States Attorney Roger B. Handberg, along with Special Agent in Charge Darrell Waldon for the IRS - Criminal Investigation Washington D.C. Field Office, and Special Agent in Charge David Walker for the FBI - Tampa Division, today announced the seizure of the SSNDOB Marketplace, a series of websites that operated for years and were used to sell personal information, including the names, dates of birth, and Social Security numbers belonging to individuals in the United States. The SSNDOB Marketplace has listed the personal information for approximately 24 million individuals in the United States, generating more than $19 million USD in sales revenue.





Account Takeover Fraud – The Schemes

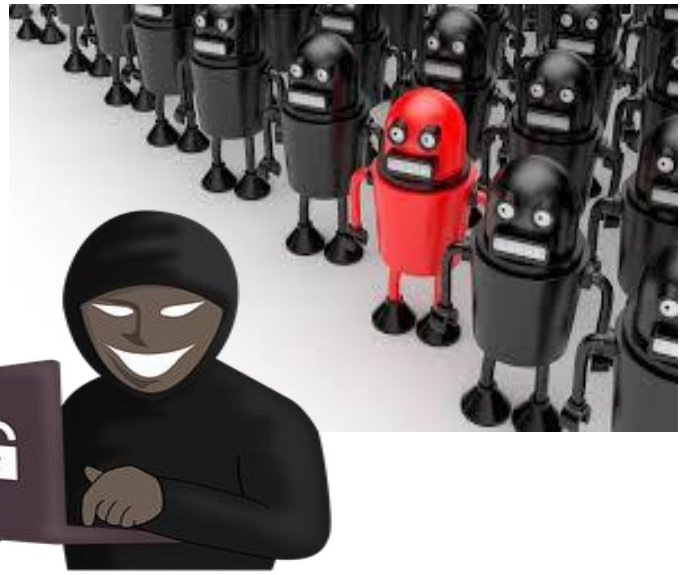
Call Center Attacks CSR's and IVRs



Agent and Impersonations



Online and BOT Attacks



Email Takeover



Employee and Fraudster Collusion



Account Takeover Fraud – The Schemes



Call Center Attacks

- Smash and Grab
- Reconnaissance
- Setting the Stage

2022 YTD by The Numbers

35% of Attacks Targeted the Call Center

- 47% Accessed Account
- **$185k** Avg. Balance Targeted
- **$74k** Avg. Withdrawal Requested
- 37% Detected by Employee
- 42% Detected by Automated Tools

Fraudsters Know Your Procedures and Are Prepared

LIMRA LOMA

Account Takeover Fraud – The Schemes



Email Takeover

- Use Customers Email to Access Their Account
- Fraudsters Learn Allot in Your Email
- Very Difficult to Defend Against

2021 ICS Data

- 19,954 BEC/EAC scam complaints
- Average loss $120,074 (+25%)
- BEC/EAC accounted for the largest percentage (35%) of financial losses related to cyber-crime

From: [redacted]
Sent: Tuesday, September 13, 2022 3:17 PM
To: [redacted]
Subject: Re: Partial Withdrawal for [redacted], Health Challenge

Hi [redacted],

Kindly say a prayer for me, This might come as a shock to you, I have been battling with larynx throat cancer for a while but have been keeping it under wraps, I have done series of chemotherapy which has been draining and making me weak, It went for a while but came back in full blown last week as i was coughing blood constantly and my throat was swollen and have not been able to talk since yesterday because am always coughing blood when i try to talk, I was advise by my doctors that i will need to go for an emergency surgery to remove the cancerous tumors and repair my voice box. My insurance company is refusing to pick up the cost because it's a clinical trial surgery and i have to pay for my surgery cost from my pocket pending when i sort it out with them, i want to request for $48,000 to pay for my surgery cost and post surgery expenses.
I will like the withdrawal deposited into my new checking account. Kindly email me the necessary paper work i need to fill.

Thank you
[redacted]

Don’t Click That Link or Open That Document

Account Takeover Fraud – The Schemes

Online Attacks

- Unregistered Online Accounts Easy Targets
- Forgot Username\Password Backdoor
- One Time Passcodes Can be Beat

BOT Attacks

- Abundance of Available Credentials
- Fraudsters can “test” unlimited #’s
- Access the Account and\or Sell Enriched Data

2022 YTD by The Numbers

60% of Attacks Targeted the Online Portals

- 69% Accessed Account
- **$224k** Avg. Balance Targeted
- **$46k** Avg. Withdrawal Requested
- 37% Detected by Customer
- 47% Detected by Automated Tools



Don’t Repeat Usernames and Passwords | Avoid Using Email as Username
Register Online Accounts and Take Full Advantage of all Security Features (OTPs)

LIMRA LOMA

Account Takeover Fraud – The Schemes



Agent Impersonations

- The Most Consequential
- Agents Can be “The Weakest Link”

2:00pm Friday
Fraudster Calls Help Desk to Reset Password and told he needs his Agent ID, then hangs up.

2:06pm Friday
Fraudster Calls Agent Benefits Department and gets Agent ID.

2:15pm Friday
Fraudster Calls Help Desk and uses agent ID to Reset Password

2:30pm Friday
Fraudster Access Agent Portal and downloads Book of Business Report

3:00pm Friday
Fraudster Starts Calling Customer Call Center requesting withdrawals

Account Takeover Fraud – The Schemes



Employee and Fraudster Collusion

- Very Difficult to Prevent and Detect
- Fraudster gets access to Everything
  - Customer Data
  - Procedures and Controls
  - Instructions



Is your employee settling gambling debts with your data?

Account Takeover Fraud – Meet the Fraudsters

The Yahoo Boys

- Yahoo means internet scam in Nigerian



Sakawa Boys

- Ghanaian term for criminals who blends interne
  based fraud with black magic rituals

EFCC Arrests 60 at Yahoo Boys' Awards Night



Operatives of the Lagos Command of the Economic and Financial Crimes Commission, EFCC, have arrested 60 suspected internet fraudsters during an awards ceremony at the Conference Hotel in Abeokuta, Ogun State.

The event tagged "Peer Youths Awards", investigation revealed, was organized to reward high-level internet fraudsters.

Items recovered from the suspects at the point of arrest include exotic cars, electronic devices, laptop computers and mobile phones.

Account Takeover Fraud – Meet the Fraudsters



"Instead of selling drugs on street corners, gang members are costing Americans millions by using personal data stolen by Russian cybercriminals to maintain fancy lifestyles." Forbes Feb. 19 2022

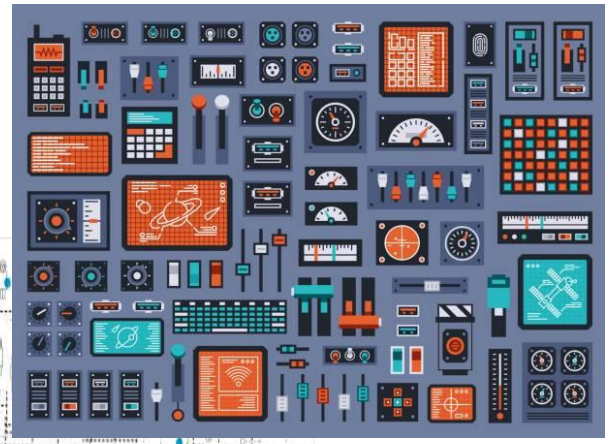
Los Angeles Times

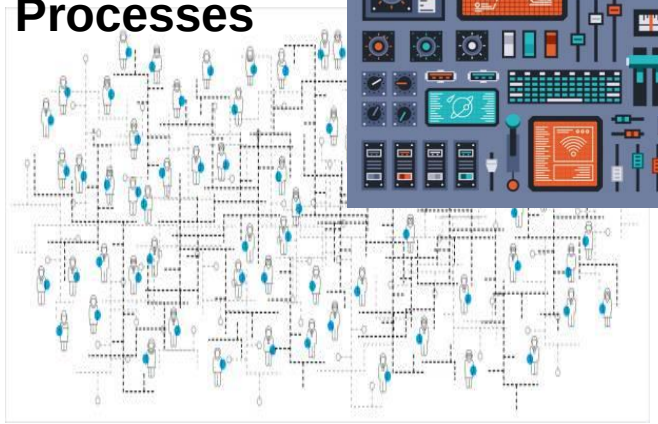
Identity theft is soaring in California, and street gangs are angling for a piece of the action.

Recent cases point to an interest in identity fraud by organizations as diverse as a Long Beach chapter of the Crips, the Armenian Power gang and the prison-based Mexican Mafia, according to law enforcement officials and fraud experts. Los Angeles Times Aug. 12, 2008

Account Takeover Fraud – Mitigation

Initial Industry Response
More Controls
More Processes





There's No Silver Bullet



Understand Your Risk Profile and Appetite



It Takes a layered Approach

- Anomaly Detection
- Disbursement Controls
- Training & Education
- Authentication
- ID Proofing

LIMRA LOMA

Account Takeover Fraud – The Opportunity

Reduced Unit Cost Through:

- Reduced Call Center Handle Times
- Reduced Back Office Processing
- Increased Self Service Capabilities
- Expanded Digital Capabilities



Improved Customer Experience Through:

- Faster Turnaround Times
- Fewer Touchpoints
- Service when customers want it and how they want it



Reliable and Effective Authentication Prevents Fraud

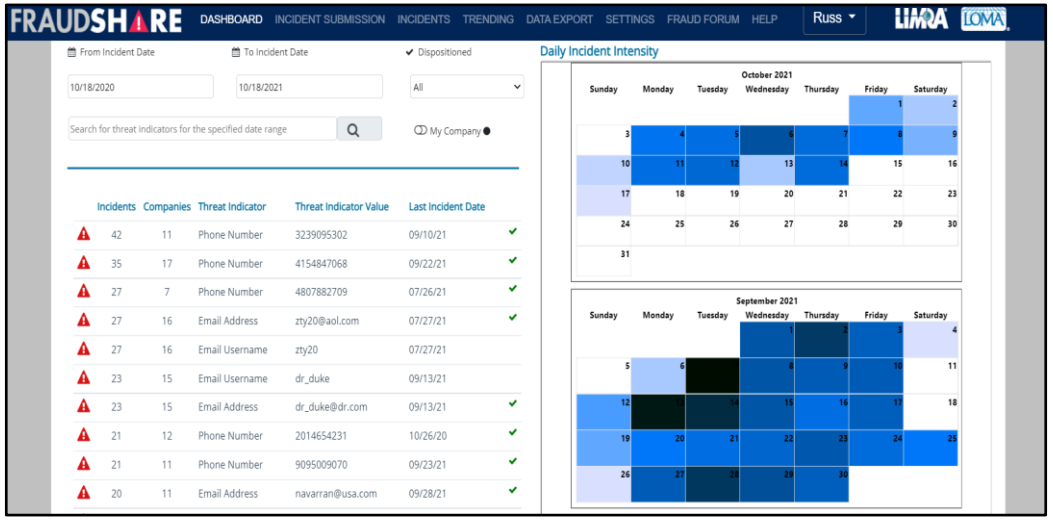


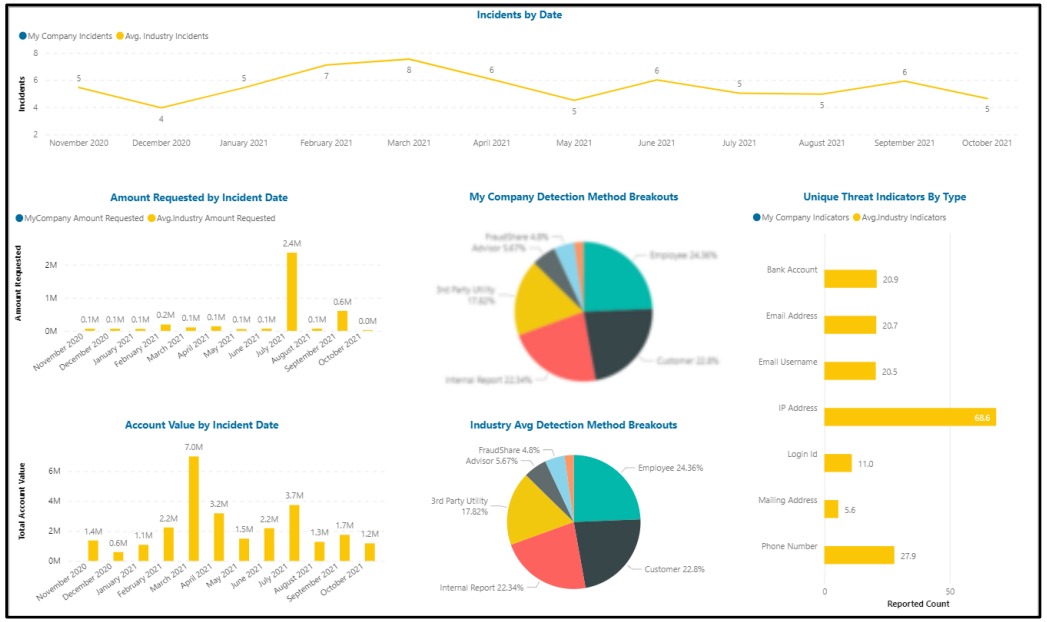
When done right fraud prevention improves the customer and company experience

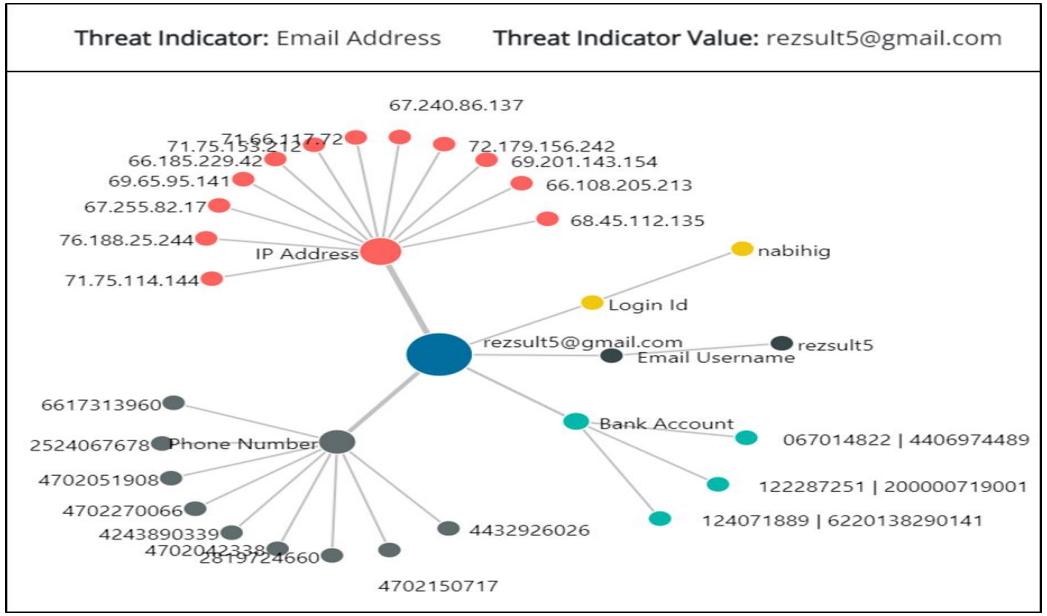
Account Takeover Fraud – FraudShare

FraudShare

- Developed by the Industry for Industry
- Access Industry Level Incident Data
- Access Threat Indicators
- Enables Collaboration to Prevent ATO







Account Takeover Fraud

Thank You

Any Questions?

Contact Info:
Russell Anderson, CFE
Randerson@LIMRA.Com
860.298.3815