RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: IDY-W12

How the H@ck R U?
A Modern Identity Assurance Approach in a Hacked World

Angel Grant, CISSP

Director, Identity, Fraud & Risk Intelligence
RSA
@AngelsGrant

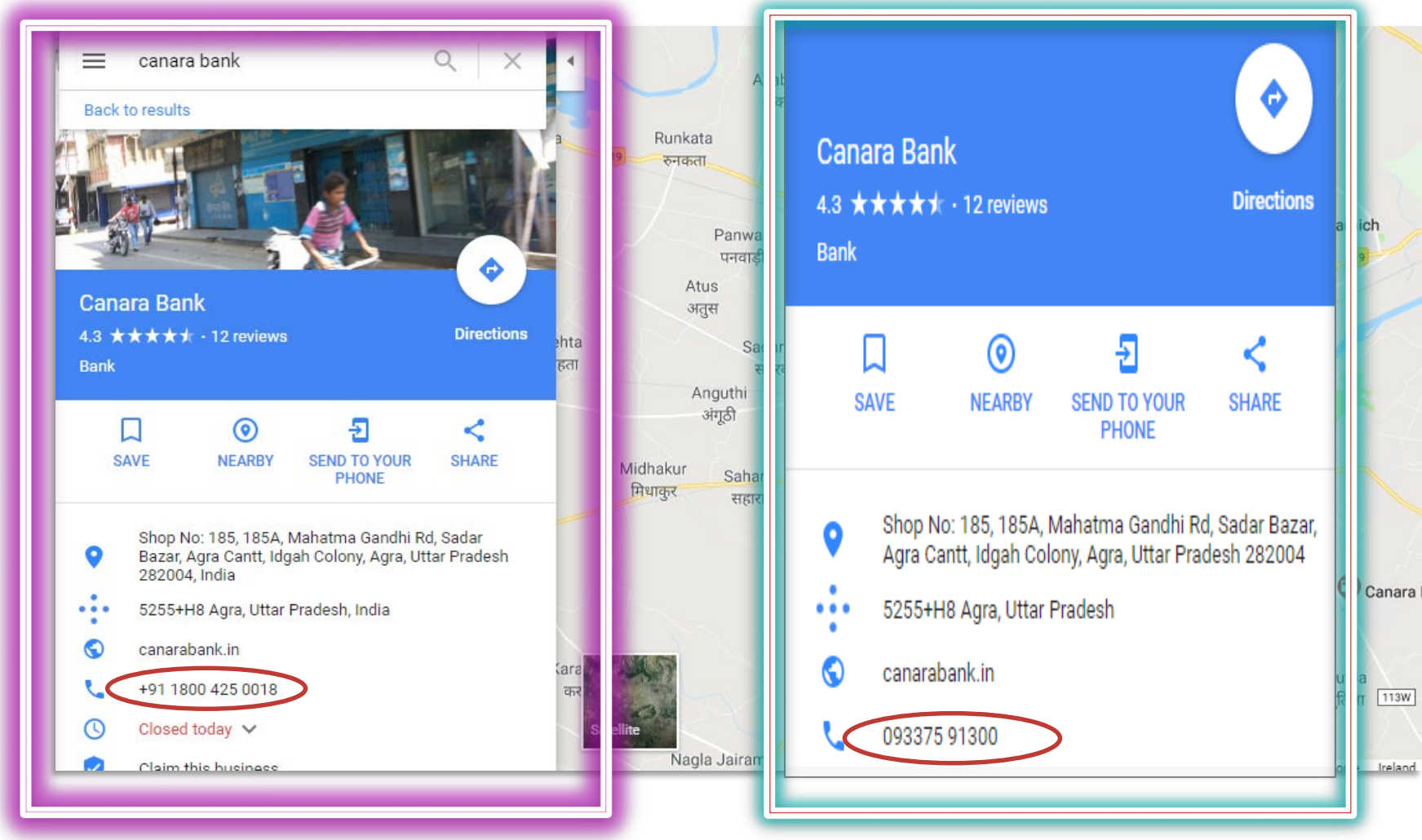

Criminal
Nation State
Hacktivist
GRAY WEB
Hiding in Plain Sight
DEEP WEB
Closed Network
DARK NET
Anonymous Network

Think Like a Cybercriminal

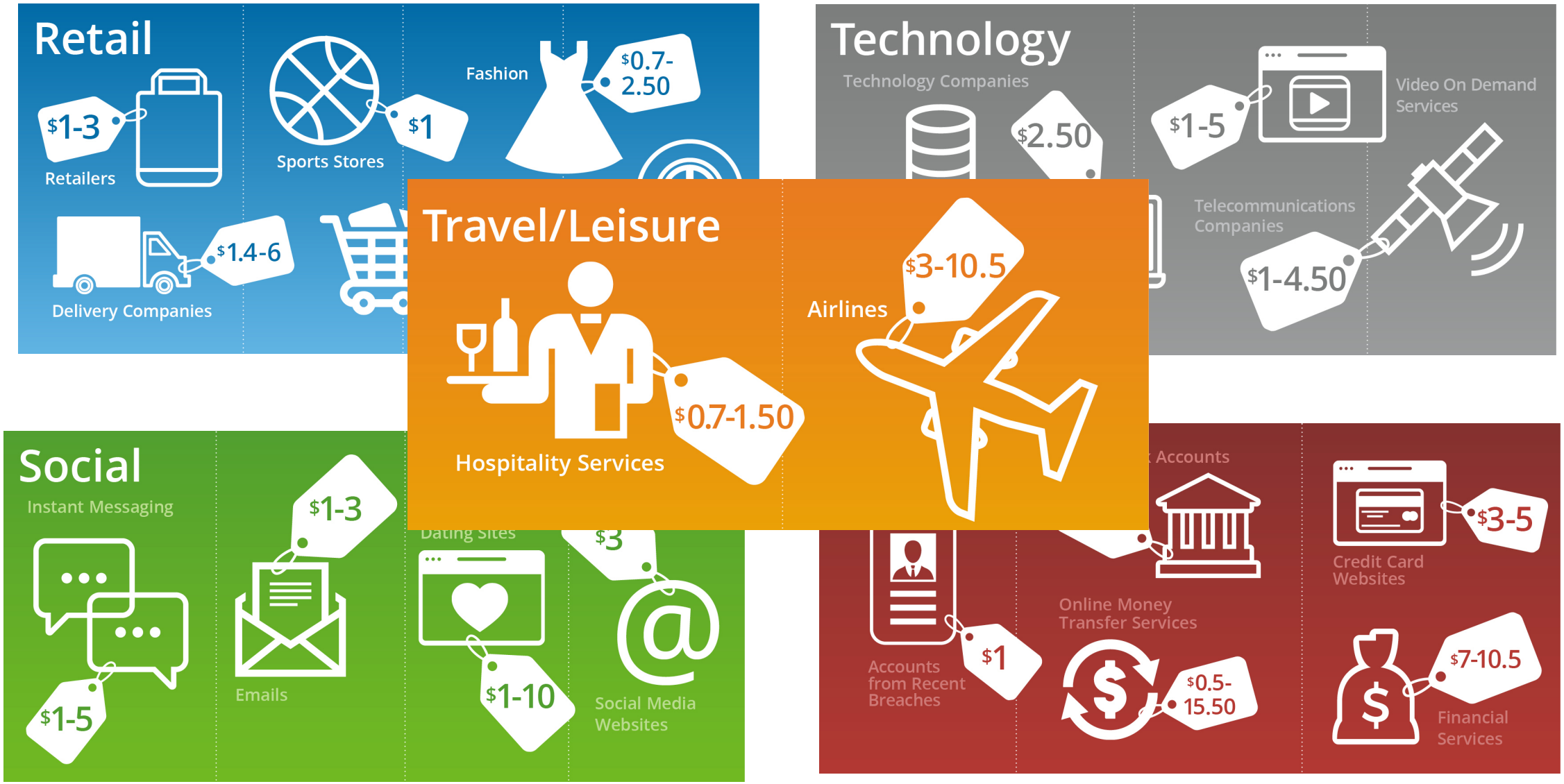
Services Offering	=	Cybercriminal Opportunity
Next-day shipping / In-store pickup	→	My shipping mule will have it before your fraud team knows its gone!
Real-time payments	→	I'll cash out before your customer calls about a weird transaction
$10 for new accounts promotion	→	One sounds good but 6,000 sounds great
"Forgot my password" link	→	Hmm…we have credential stuffing tools
Account locks after 5 failed logins	→	Good luck making $ when I lock your users
Aggregated online accounts	→	Cool, identity theft one-stop-shop!

Here is How a Cybercriminal Thinks - Vishing in Reverse

- Customer searches for phone number
- Google Maps present details
- Customer calls fraudster

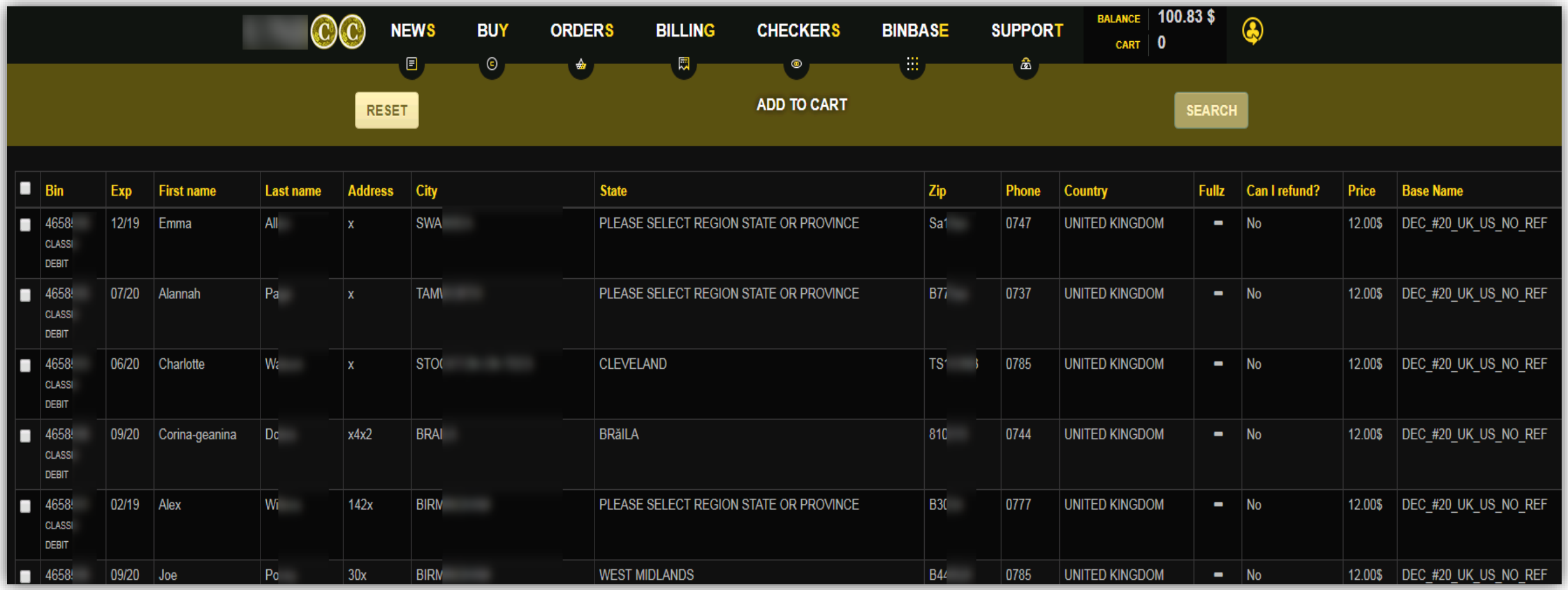


Why Cybercriminals Target Specific Industries



*Source www.rsa.com/fraudprevention

Customizable Shopping - CVV Store



Bin	Exp	First name	Last name	Address	City	State	Zip	Phone	Country	Fullz	Can I refund?	Price	Base Name
4658 CLASSI DEBIT	12/19	Emma	All	x	SWA	PLEASE SELECT REGION STATE OR PROVINCE	Sa	0747	UNITED KINGDOM	-	No	12.00$	DEC_#20_UK_US_NO_REF
4658 CLASSI DEBIT	07/20	Alannah	Pa	x	TAM	PLEASE SELECT REGION STATE OR PROVINCE	B7	0737	UNITED KINGDOM	-	No	12.00$	DEC_#20_UK_US_NO_REF
4658 CLASSI DEBIT	06/20	Charlotte	W	x	STO	CLEVELAND	TS	0785	UNITED KINGDOM	-	No	12.00$	DEC_#20_UK_US_NO_REF
4658 CLASSI DEBIT	09/20	Corina-geanina	Dc	x4x2	BRAI	BRăILA	810	0744	UNITED KINGDOM	-	No	12.00$	DEC_#20_UK_US_NO_REF
4658 CLASSI DEBIT	02/19	Alex	Wi	142x	BIRM	PLEASE SELECT REGION STATE OR PROVINCE	B30	0777	UNITED KINGDOM	-	No	12.00$	DEC_#20_UK_US_NO_REF
4658	09/20	Joe	Po	30x	BIRM	WEST MIDLANDS	B44	0785	UNITED KINGDOM	-	No	12.00$	DEC_#20_UK_US_NO_REF

Shopping for Credentials on Account Stores

HOME | ACCOUNTS | STUFF | TUTORIALS | CARDS | PURCHASED | REPORTS | RULES | REFILL BALANCE | PROFILE | SUPPORT | SELLER | S. RANKINGS

ACCOUNTS

Use search box, to search for sellers,information etc.

Type: Any | Country: Any | Seller: Any

Any | Match | ChristianMingle | POF | Jdate | Eharmony | Zoosk | FirstMet | Chemistry | MuslimMatch | SingleParentMeet | Mingle2

CHEAPEST

Search:

- Any
- BeNaughty(Unpaid)
- MeetMe(UnPaid)
- BlackPeopleMeet(Unpaid)
- ChristianMingle(UNPAID)
- POF(PAID)
- FirstMet(UNPAID)
- Seniorpeoplemeet(UNPAID)
- Mingle2(UNPAID)
- SeekingArrangemen(Unpaid)
- Match(PAID)
- (PAID)
- POF(Unpaid)
- Okcupid(UNPAID)
- Ourtime

Information	Seller	Price	
Friends Count: 0 // Credit Balance: 0 // NAME : : Ward // Gender: m // Province : NY		3.00$	
PAID Pof - Gender: Male, Age: 21, Profile: www.pof.com/viewprofile.aspx?profile_id=, Subscription Status: 3 Month Upgrade, Expire: 2017-06-18		10.00$	Buy
Unpaid Account - Wheeling, IL / Age: 75 / DOB: January/ /1942 / Male		4.00$	Buy
UNPAID Match - Country: United-States, Age: 21, Gender: Male, Zip Code: 90706		2.99$	Buy
UNPAID Match - Gender: Female, Age: 26, Country: United-States, Zip: 56556, DOB: .08.1990		3.00$	Buy
UNPAID - Birthday: 1962-11-2 T00:00:00.000Z, Gender: MALE, Country: US		3.00$	Buy
Free Account / Female / Zip Code: 12912 / September-4-1992 / Age: 25 / United States / a s / New York		3.00$	Buy

Thursday 25 January 2018

News Crime

FOLLOW | CONTACT

Romance fraud: Irish woman lost €37,000 after falling in love with a man claiming to be a US soldier serving in Afghanistan

Victims fall in love with what they believe are their perfect partners online – until they discover they have been scammed into handing over a substantial amount of money to help solve a financial problem – in what is known as a 'catfish' scam. Stock picture

Tom Brady
January 23 2018 11:51 PM

ROMANCE fraud is blooming on the internet and is becoming a worrying problem for members of the Garda National Economic Crime Bureau, who say it is on the increase here.

Victims fall in love with what they believe are their perfect partners online – until they

Most Read | Most Shared

- 'No way' jailed brother will be released for funeral of latest Hutch-Kinahan feud... Crime
- Romance fraud: Irish woman lost €37,000 after falling in love with a man claiming to be a US... Crime
- Brother of feud murder victim Derek Coakley Hutch heard him being shot dead via a... Crime
- Gardai arrest man in connection with serious assault that left 35-year old in critical... Crime
- Pictured: Third nephew of Gerry 'The Monk' Hutch killed in gangland shooting Crime

The Daily Digest

Today's news headlines, directly to your inbox every morning.

Email address | Sign Up

Promoted Links by Outbrain

- How a Canadian City Ended Homelessness With a Simple Idea — Goodnet
- Sir Cliff Richard Knocks €3 Million Off Portuguese Vineyard Estate — Mansion Global

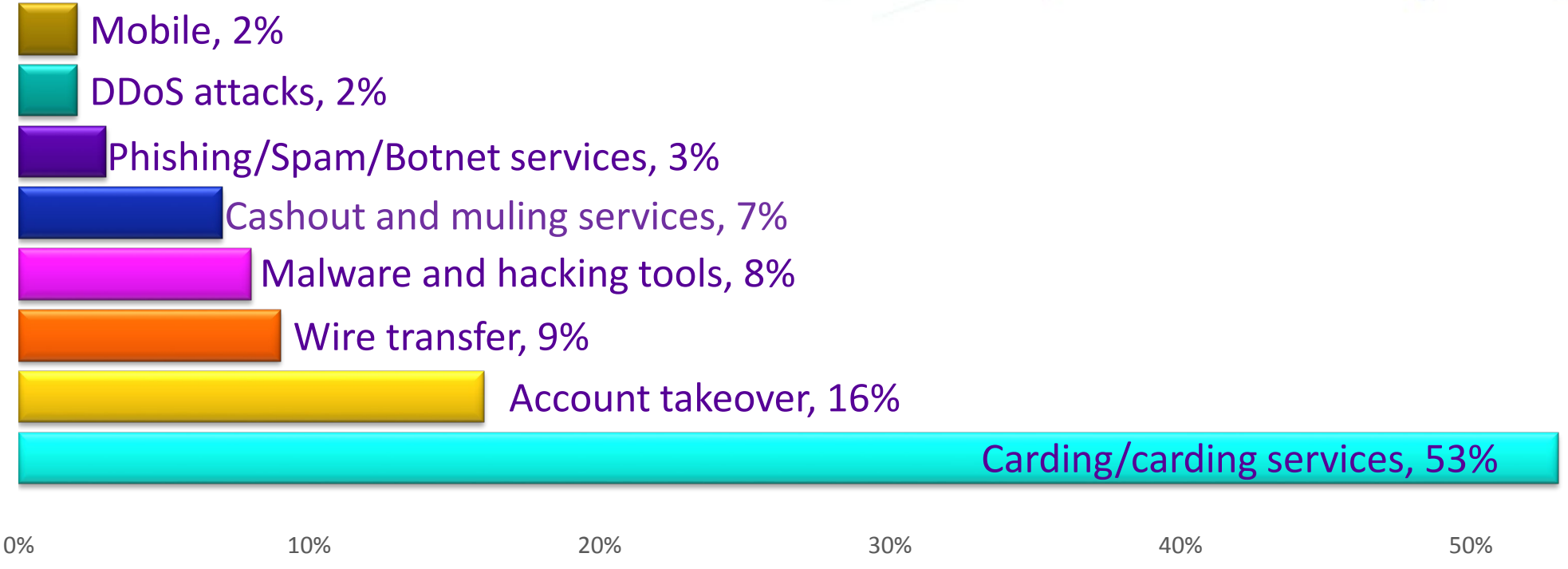
One Stop Simplified Cybercrime Shops

Name: [redacted] Category: Dedicated servers (RDP) USA 240 13973 100 98 11 Sort by

You can subscribe to the category updates. When replenishing the product, we will notify you in Jabber Subscribe

Title	Country	State	Info	Blacklist	Upload	
Dedicated server (RDP) USA and other countries	Thailand	N/A	User, Windows 2012, RAM 16.00 GB, NO Blacklist	NO	21/10/2018 22:04	+ $8.00
Dedicated server (RDP) USA and other countries	India	Delhi	Administrator, Windows 2012, RAM 64.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $10.00
Dedicated server (RDP) USA and other countries	South Africa	Gauteng	User, Windows 2008, RAM 16.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $8.00
Dedicated server (RDP) USA and other countries	Japan	Tokyo	User, Windows 2012, RAM 64.00 GB, Yes Blacklist	YES	8/10/2018 10:30	+ $8.00
Dedicated server (RDP) USA and other countries	Morocco	Grand Casablanca	User, Windows 2007, RAM 24.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $8.00
Dedicated server (RDP) USA and other countries	Germany	Niedersachsen	User, Windows 2016, RAM 4.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $8.00
Dedicated server (RDP) USA and other countries	Malta	N/A	User, Windows 2012, RAM 8.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $8.00
Dedicated server (RDP) USA and other countries	South Africa	Western Cape	User, Windows 2007, RAM 3.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $8.00
Dedicated server (RDP) USA and other countries	Kenya	Nairobi Area	Administrator, Windows 2012, RAM 64.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $10.00
Dedicated server (RDP) USA and other countries	France	N/A	User, Windows 2016, RAM 16.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $8.00
Dedicated server (RDP) USA and other countries	Netherlands	Utrecht	User, Windows 10, RAM 4.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ $8.00
Dedicated server (RDP) USA and other countries	Czech Republic	Hlavni mesto Praha	User, Windows 2012, RAM 32.00 GB, NO Blacklist	NO	7/10/2018 19:37	+ $8.00

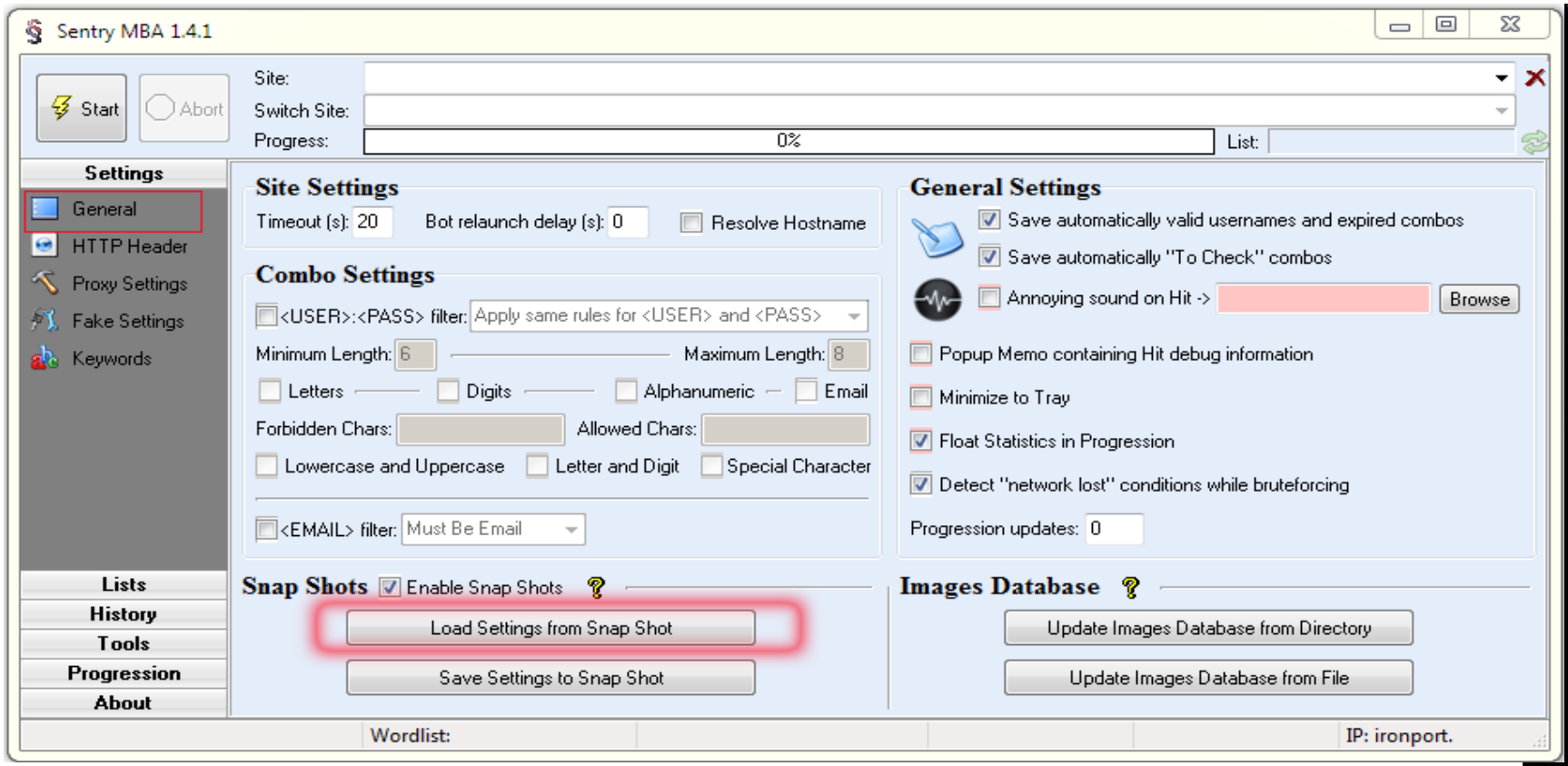
Dark Web Morphing into “Gray Web”

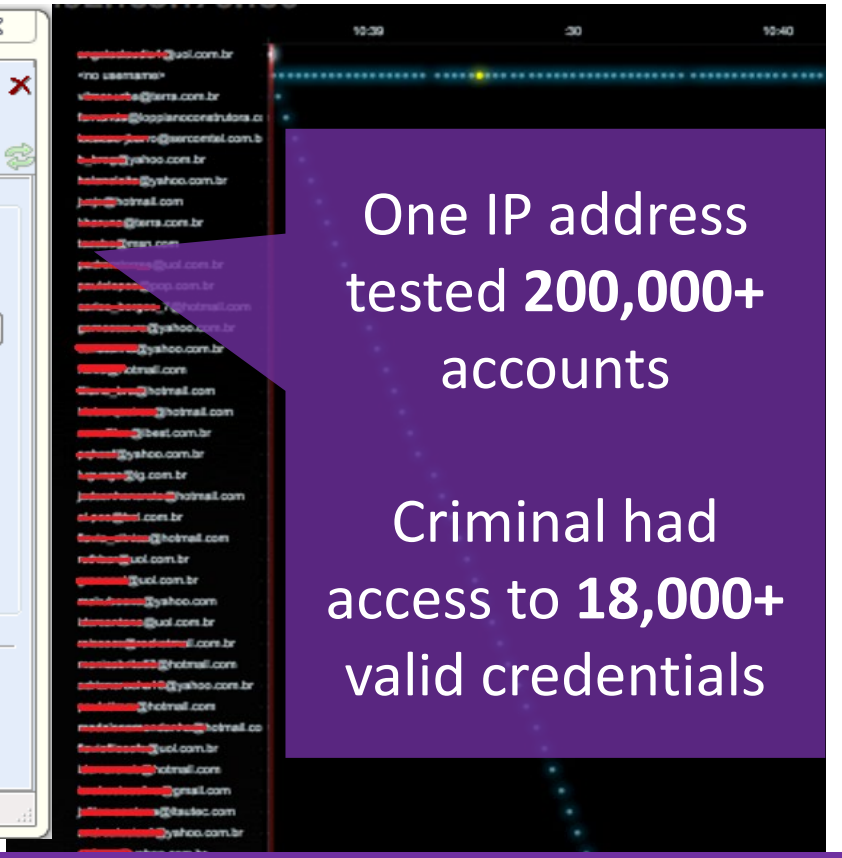


7 Regions **500 Groups** **300K Users** **300% Growth**

Surplus Inventory Selling in Plain Sight

Why Steal It When You Can Stuff It

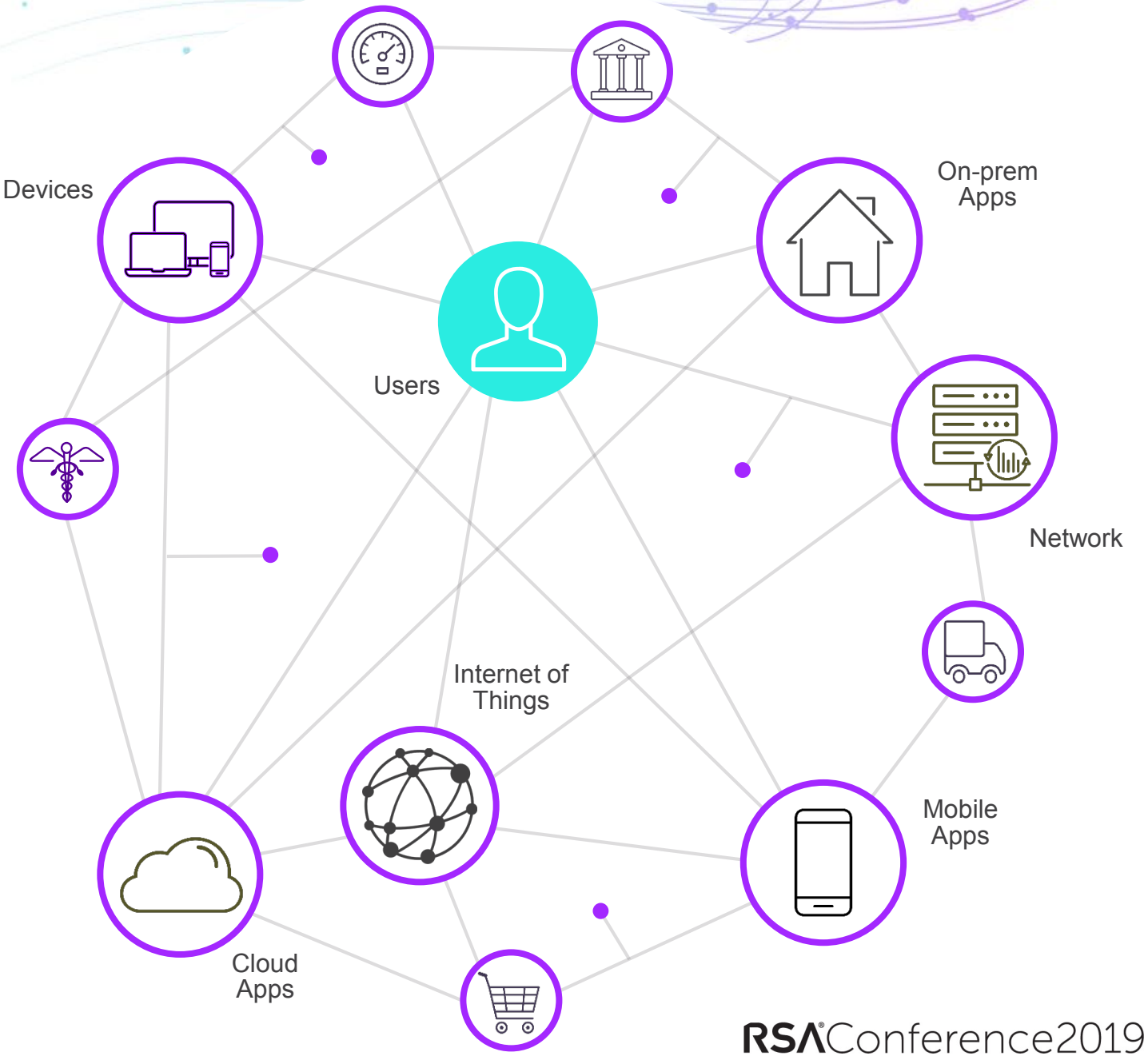




- **New Account** has **15x higher fraud** rates in **1st 10 days**
- **Fraud** rates **3x higher** from **new device**

*Source RSA Adaptive Authentication Customer Base

IDENTITY OF CONNECTED THINGS Opens Business Opportunities And Vulnerabilities



IDENTITY ASSURANCE

is the user or entity who they claim they are?

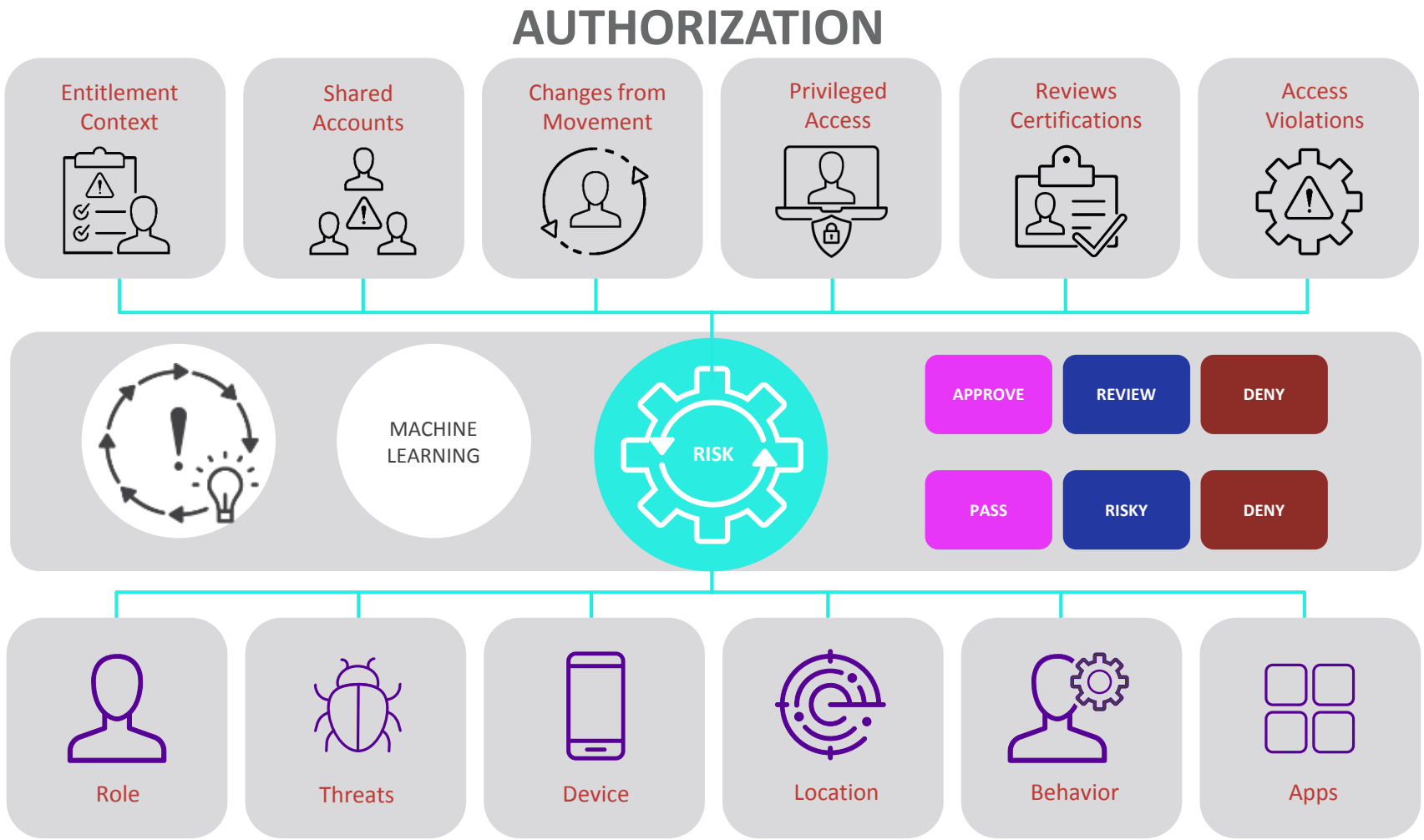
ACCESS ASSURANCE

what level of access to applications and data is ok?

ACTIVITY ASSURANCE

is what they are doing appropriate or not?

TRANSLATE VISIBILITY INTO INSIGHTS BY CORRELATING ACCESS DATA



IDENTITY & ACCESS MANAGEMENT

WHO is the user?

WHAT can they access?

IS what they are doing ok?

NETWORK & PERIMETER SECURITY

HOW do you take threats into account?

FRAUD INTELLIGENCE

WHAT known fraud is this user or device associated with?

GOVERNANCE, RISK & COMPLIANCE

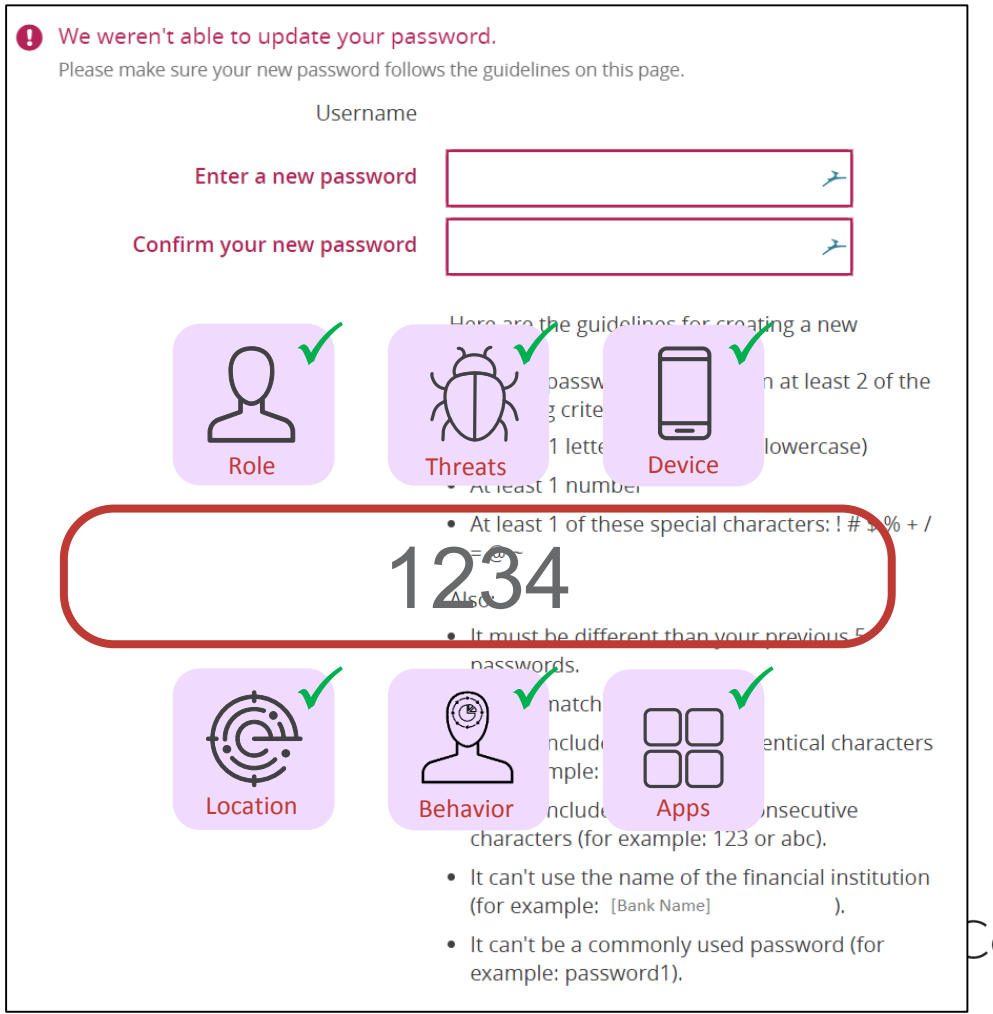
WHY should I care?

Is there a risk to my business?

Use Case #1: Identity Assurance

Trust a simple 4 digit PIN for VPN access?

Th1$2$4ck$!

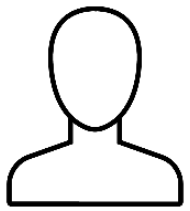


Apply Identity Analytics

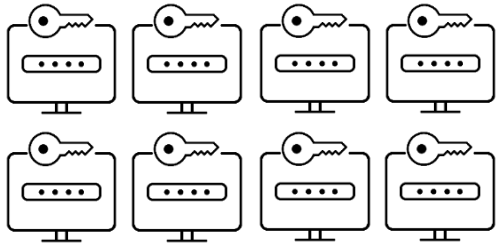
How about now?

Use Case #2: Access Assurance

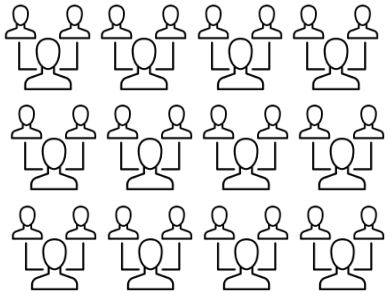
USERS



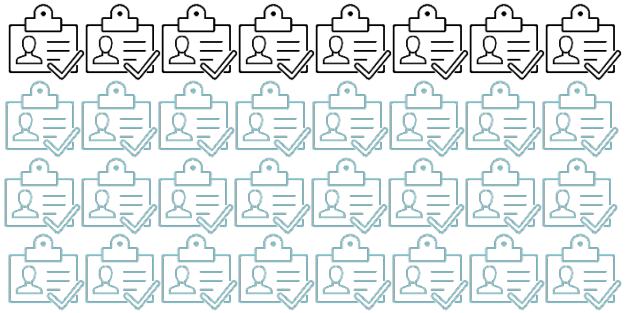
ACCOUNTS



ROLES



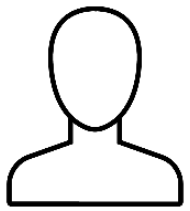
ENTITLEMENTS



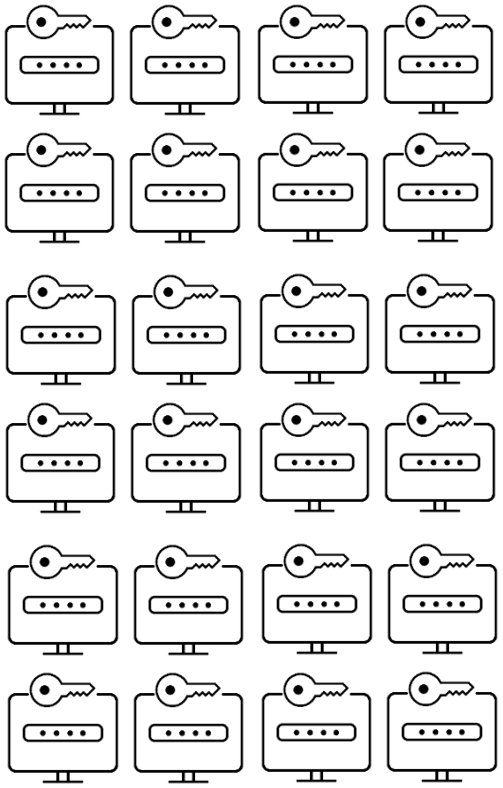
DECISION

Use Case #2: Access Assurance

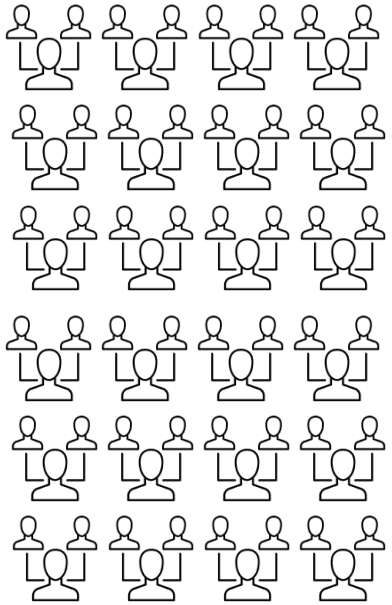
USERS



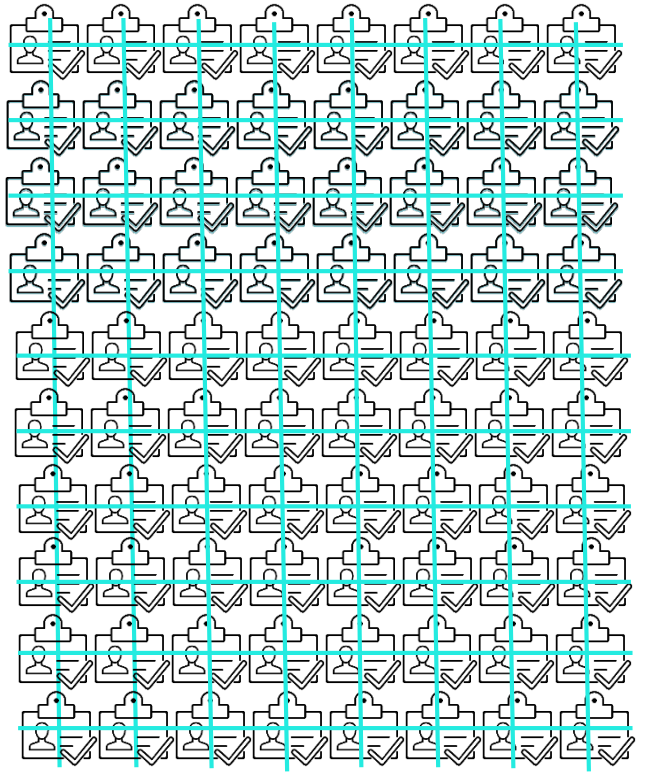
ACCOUNTS



ROLES



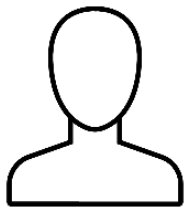
ENTITLEMENTS

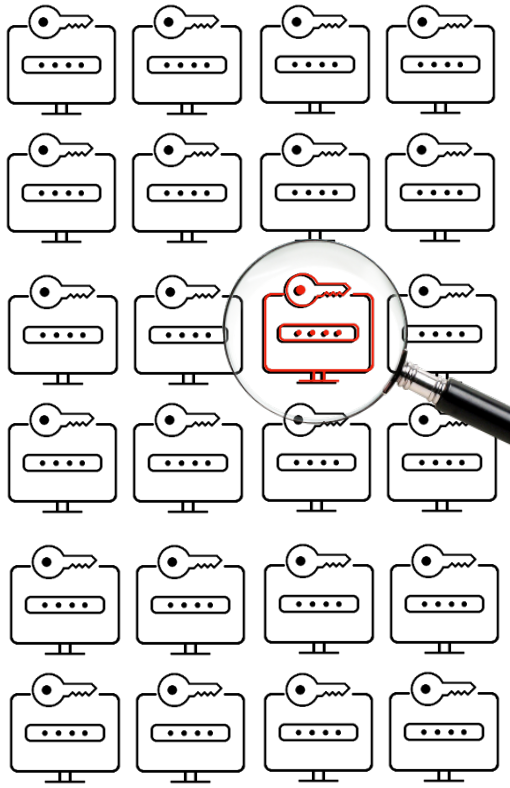


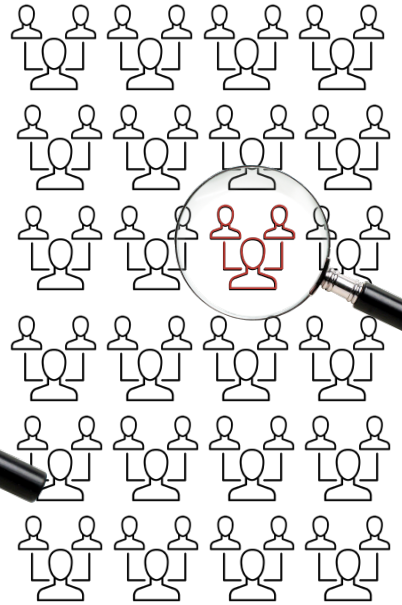
DECISION

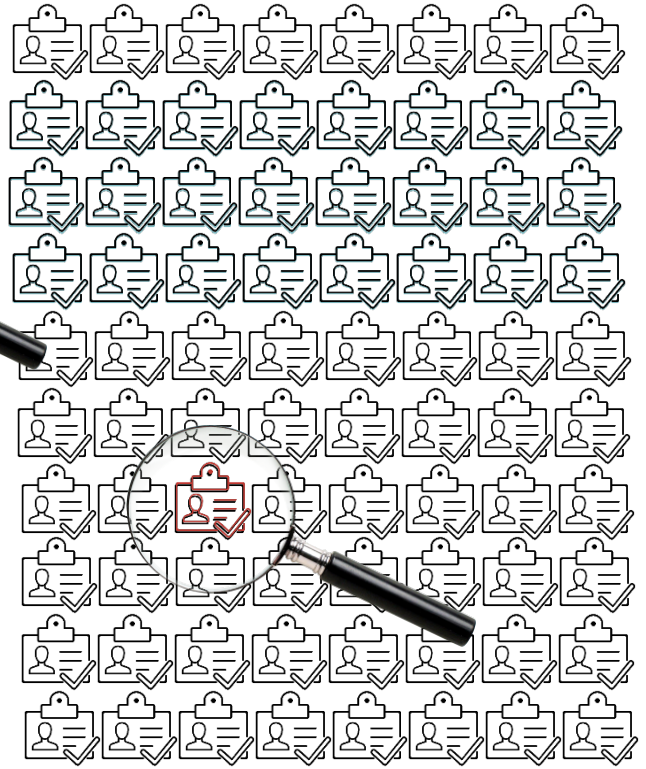
Use Case #2: Access Assurance

USERS ACCOUNTS ROLES ENTITLEMENTS DECISION

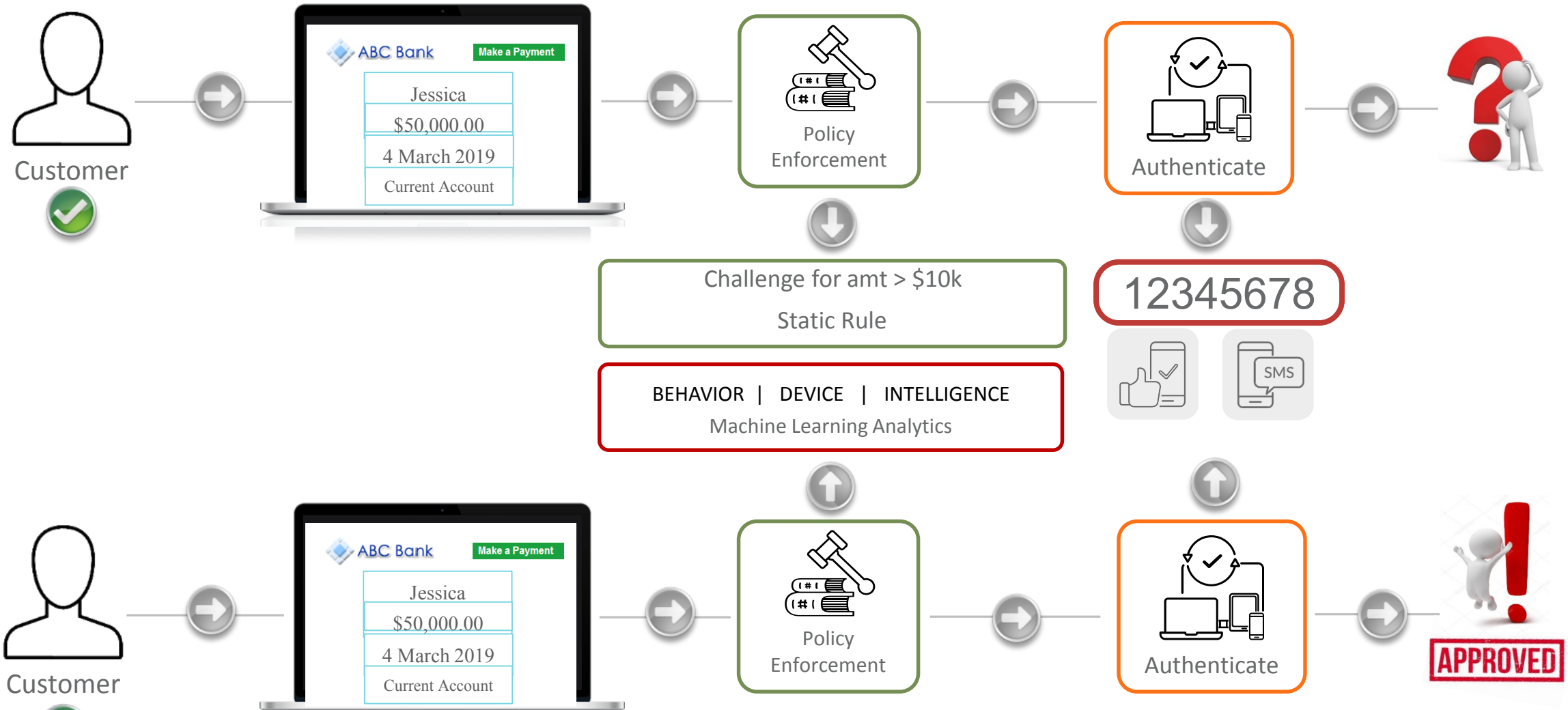




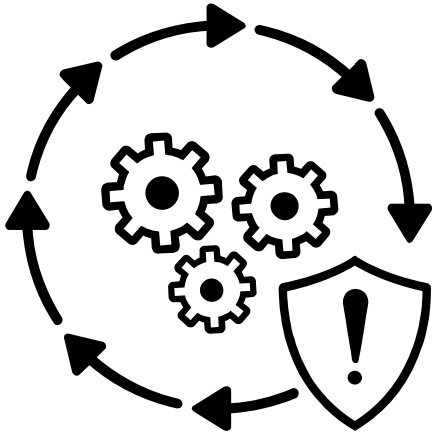




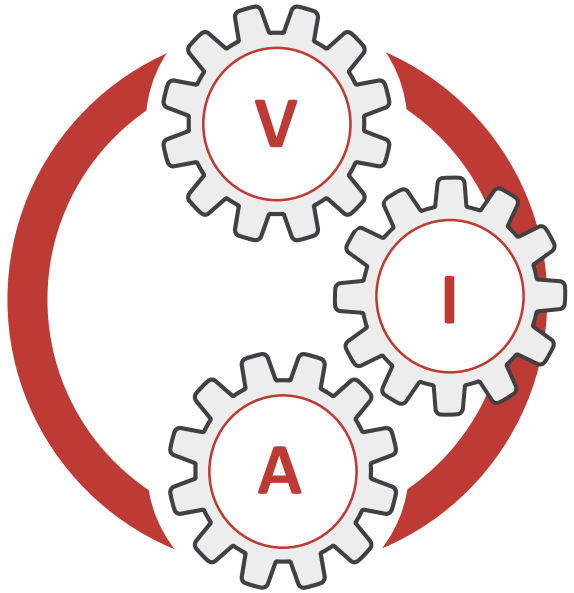
Use Case #3: Activity Assurance



What Should You Do to Transform Your Identity Assurance Strategy?



Augment static-rules with analytics



Expand visibility & insight to take Action

Harness the power across your security village

How the H@CK R U Now?

Apply What You Have Learned Today

- **Next week you should:**
  - Identify who is monitoring cybercrime underground for your company
- **In first three months you should:**
  - Investigate new potential points of vulnerably
    - (e.g. Shadow IoT, islands of identities, credentials sold on social media)
  - Create plan to mitigate account takeover
  - Augment static-based IAM rules with identity analytics
- **Within six months you should**:
  - Unite your security village
    - including threat detection, GRC and fraud prevention tools

RSAConference2019

Angel Grant, CISSP
RSA, Director
@Angelsgrant

RSA