

Balancing Risk & Reward

The New Mobile Battlefield



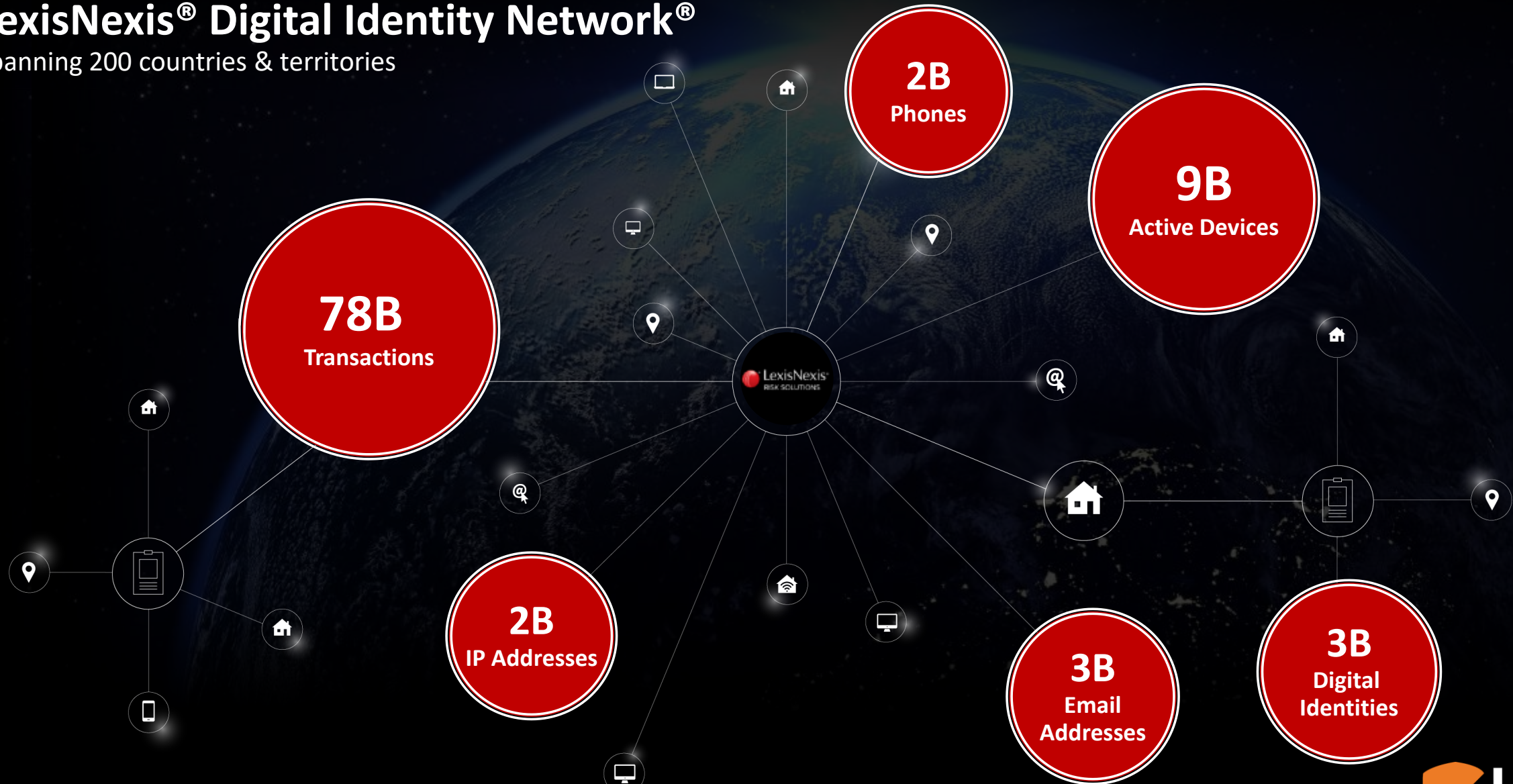
Analysis from The LexisNexis[®] Risk Solutions Cybercrime Report | July to December 2021



Jason Lane-Sellers
Director, Fraud & Identity - LNRS
President – Communication Fraud Control Association

The CCR is based on data within the LexisNexis® Digital Identity Network®

Spanning 200 countries & territories



Joint Fraud Conference

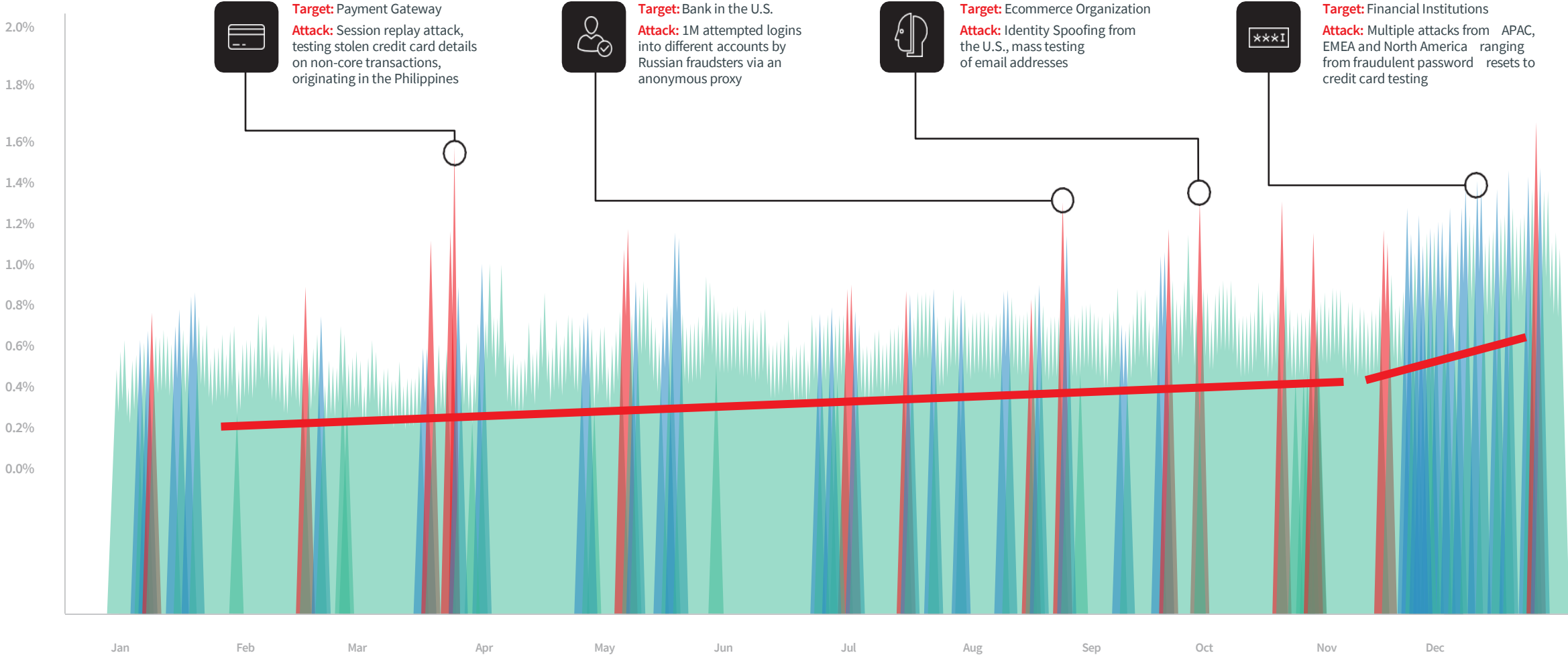


Our Contributory Network Is Almost Impossible to Replicate



Identity Abuse Index

IDENTITY ABUSE INDEX



H2 – 2021 - Data

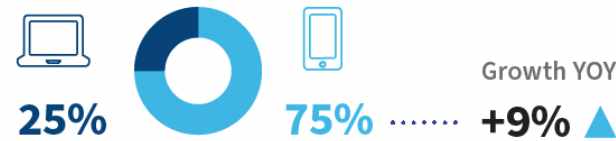
- Digital has become a focal point during and post Pandemic
- **44%** Growth in transactions YOY
- Mobile is dominating the transaction channel of choice
- Mobile APP is becoming the go to access point for the consumer
- All aspects of interactions are growing

TRANSACTIONS PROCESSED JULY-DECEMBER 2021

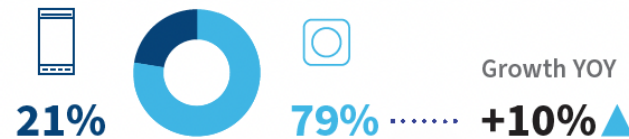
35.5B Growth YOY **+44%** ▲

TRANSACTIONS BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App

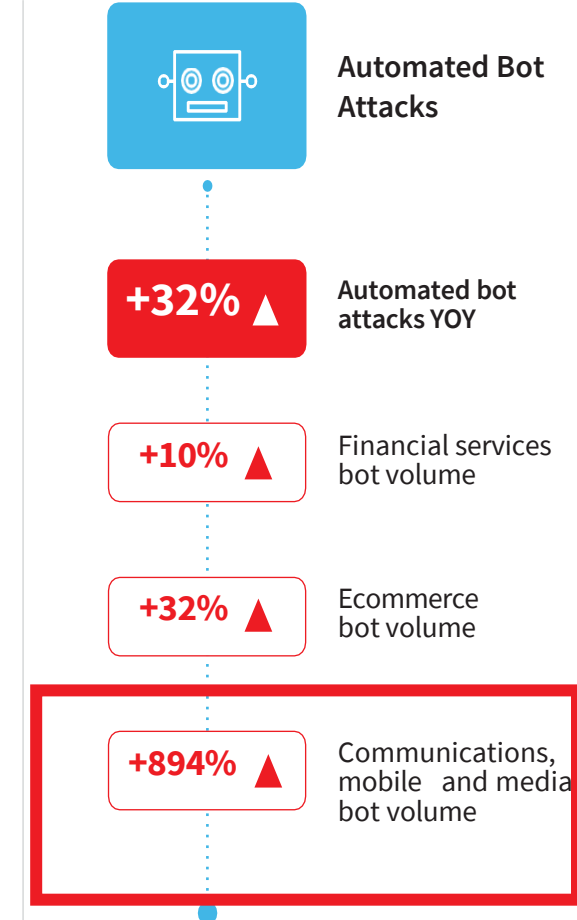
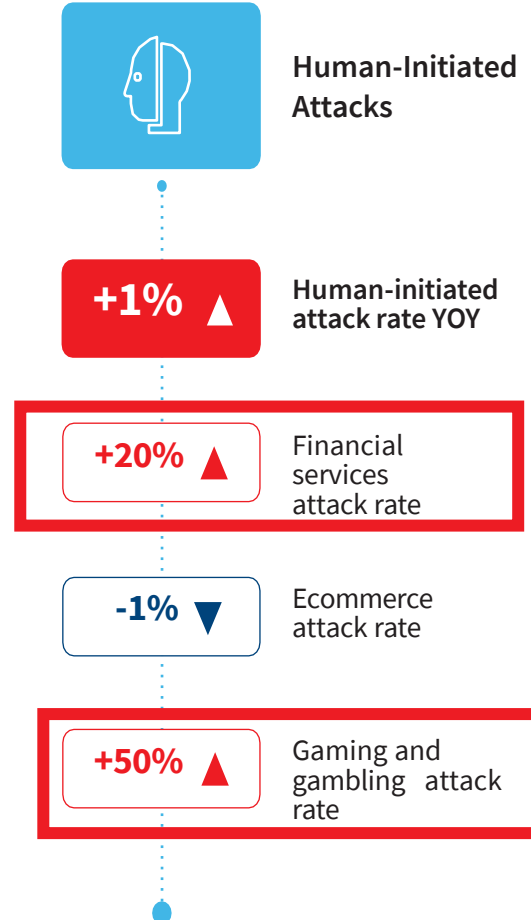
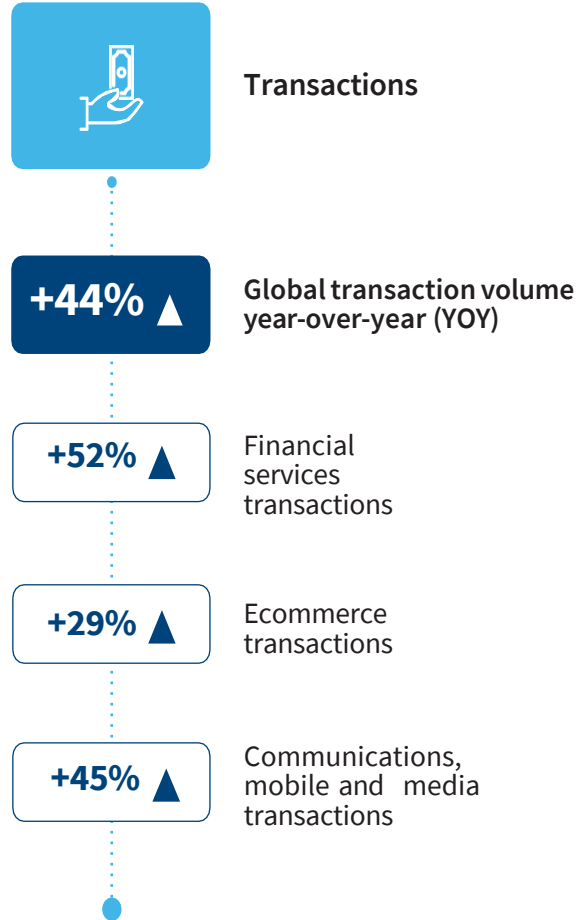


TRANSACTIONS BY USE CASE

		Growth YOY
New Account Creations	516M +4% ▲
Logins	25.7B +51% ▲
Payments	5.9B +35% ▲

H2 – 2021 - Trends

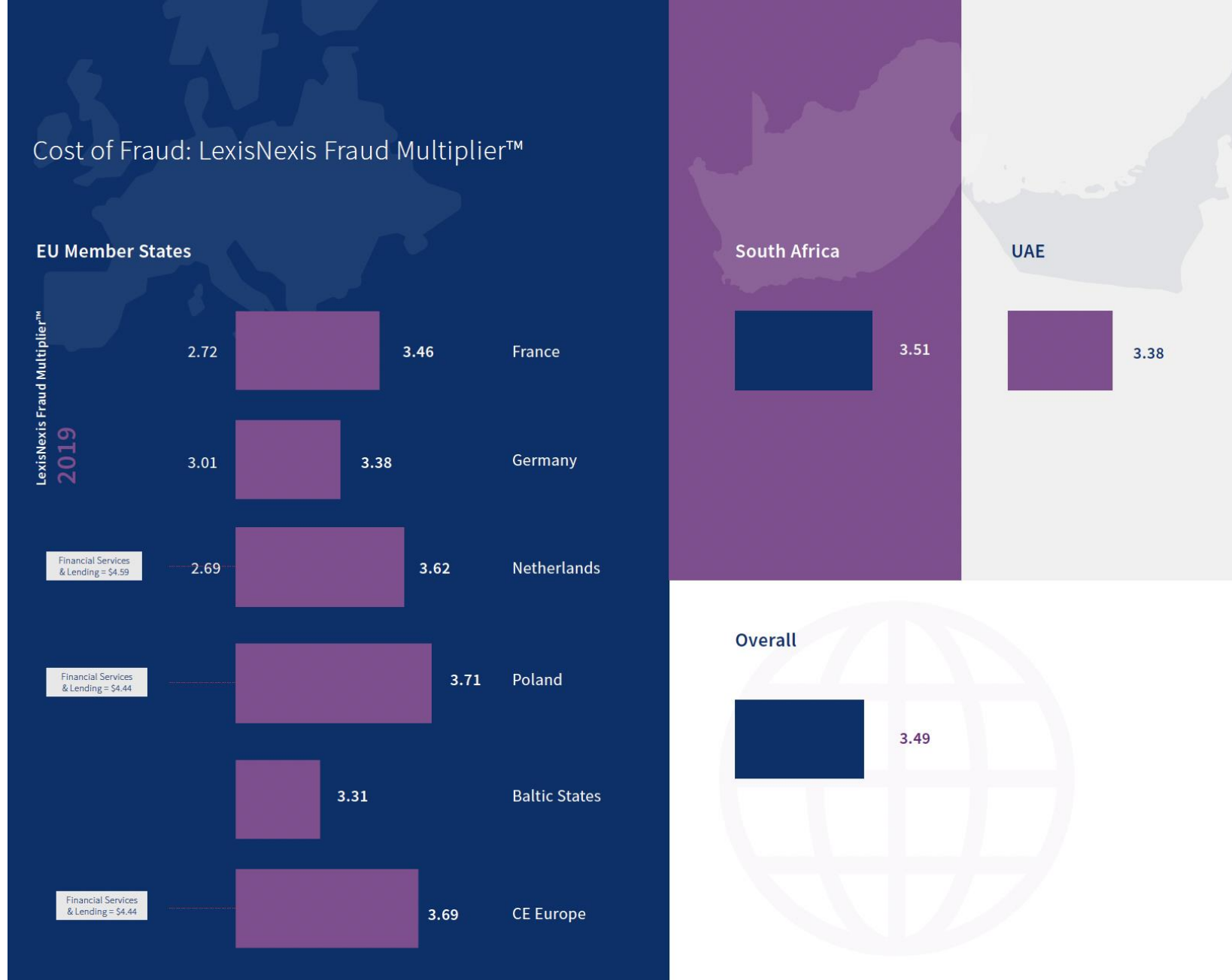
- Human initiated attacks have begun to grow again post pandemic
- Financial services and Gaming and Gambling receiving the focus for human initiated attacks
- CMM & Ecommerce the growing focus for automated attacks
- Huge escalations of attacks against CMM attempting to compromise credentials and gather data for social engineering



Fraud Cost

The 2022 Total Cost of fraud shows that:

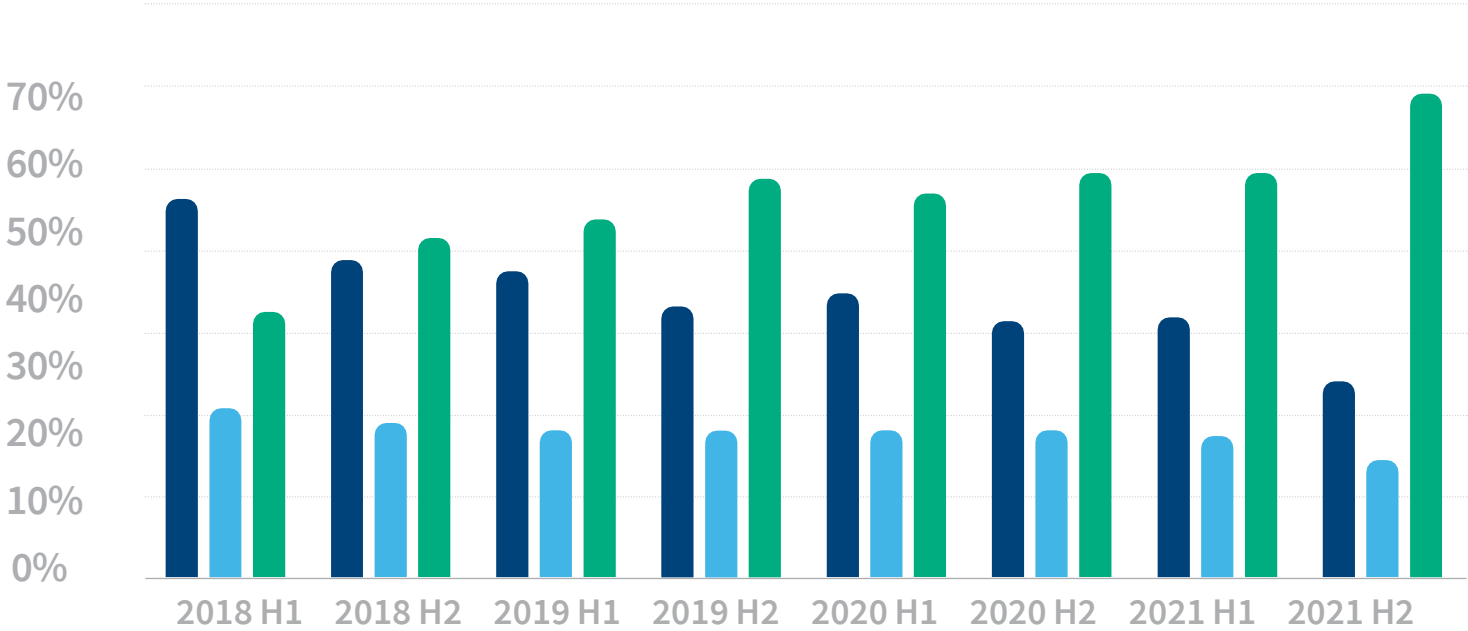
Every fraudulent transaction costs **3.49** times the lost transaction value on average.



The Rise of Mobile for Good Customers and Fraudsters

- Younger demographic has pushed adoption of mobile apps
- Mobile Browser still popular with people who do not have modern smart phones, or choose not to sign up to app based services

Transactions

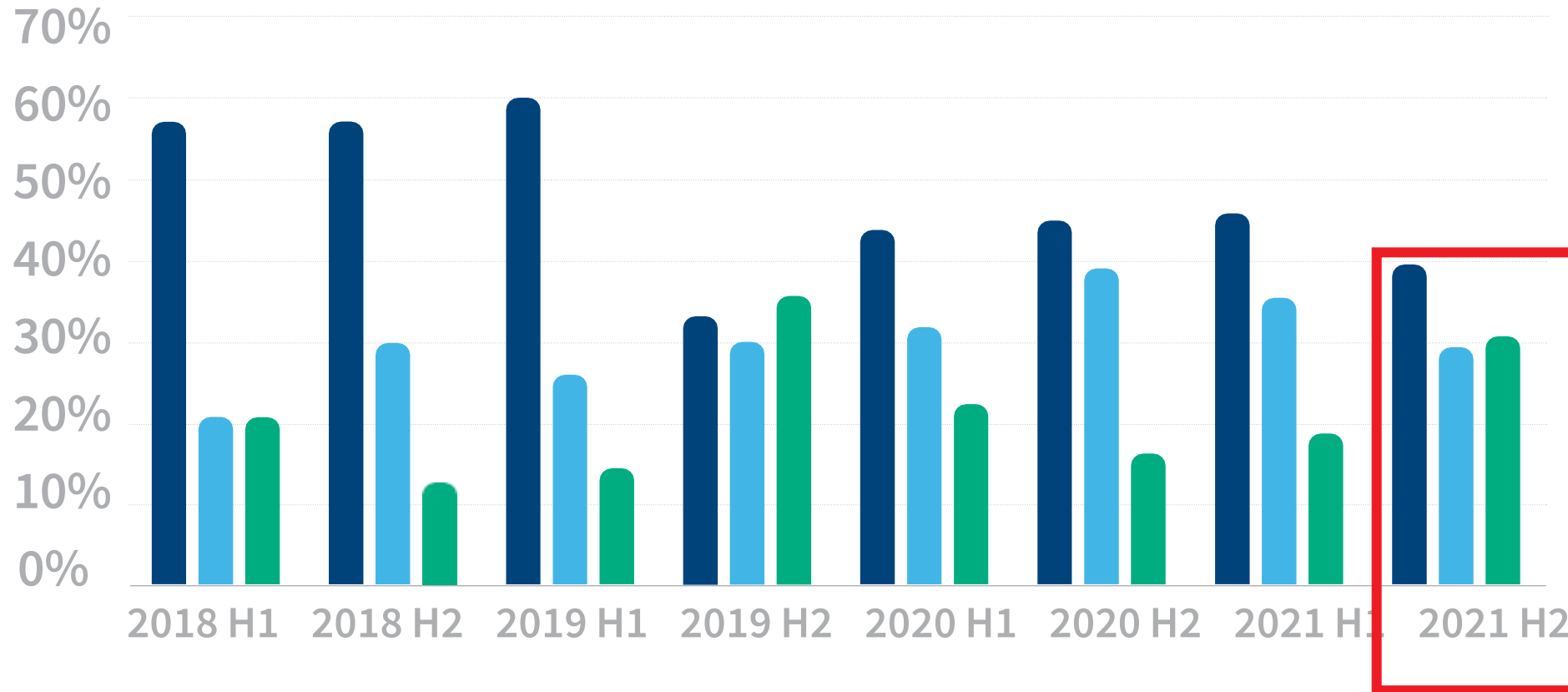


- DESKTOP
- MOBILE BROWSER
- MOBILE APP

The Rise of Mobile attacks

SHARE OF ATTACKS

- In 2018 attacks were predominantly focused on the desktop channel
- The 'safer' mobile app channel may become the most attacked channel by 2023



Human Initiated Attacks Back on the Rise



HUMAN-INITIATED ATTACKS

ATTACK VOLUME

344M

Growth YOY
+46% ▲

- As regions started to move into a post pandemic opening for service the fraudsters have immediately re-initiated attacks
- EMEA & the US have been the immediate victims from post pandemic growth in attack rates

Attack Rate by Desktop / Mobile



Percentage of attacks coming from mobile devices has **increased YOY**



ATTACK RATE

			Growth/Decline YOY
⚠️	Overall	1.1%	+1% ▲
💻	Desktop	1.8%	+12% ▲
📱	Mobile Browser	2.2%	-6% ▼
📷	Mobile App	0.6%	+59% ▲

Continual Rise of Automated Attacks






AUTOMATED BOT ATTACKS

- Automated and BOT attacks have continually grown over the past few years
- CMM and Ecommerce have been the focal for automated attacks
- CMM has been driven by two elements – credential testing for compromised details from data breaches and gathering implicit user data for social engineering scams

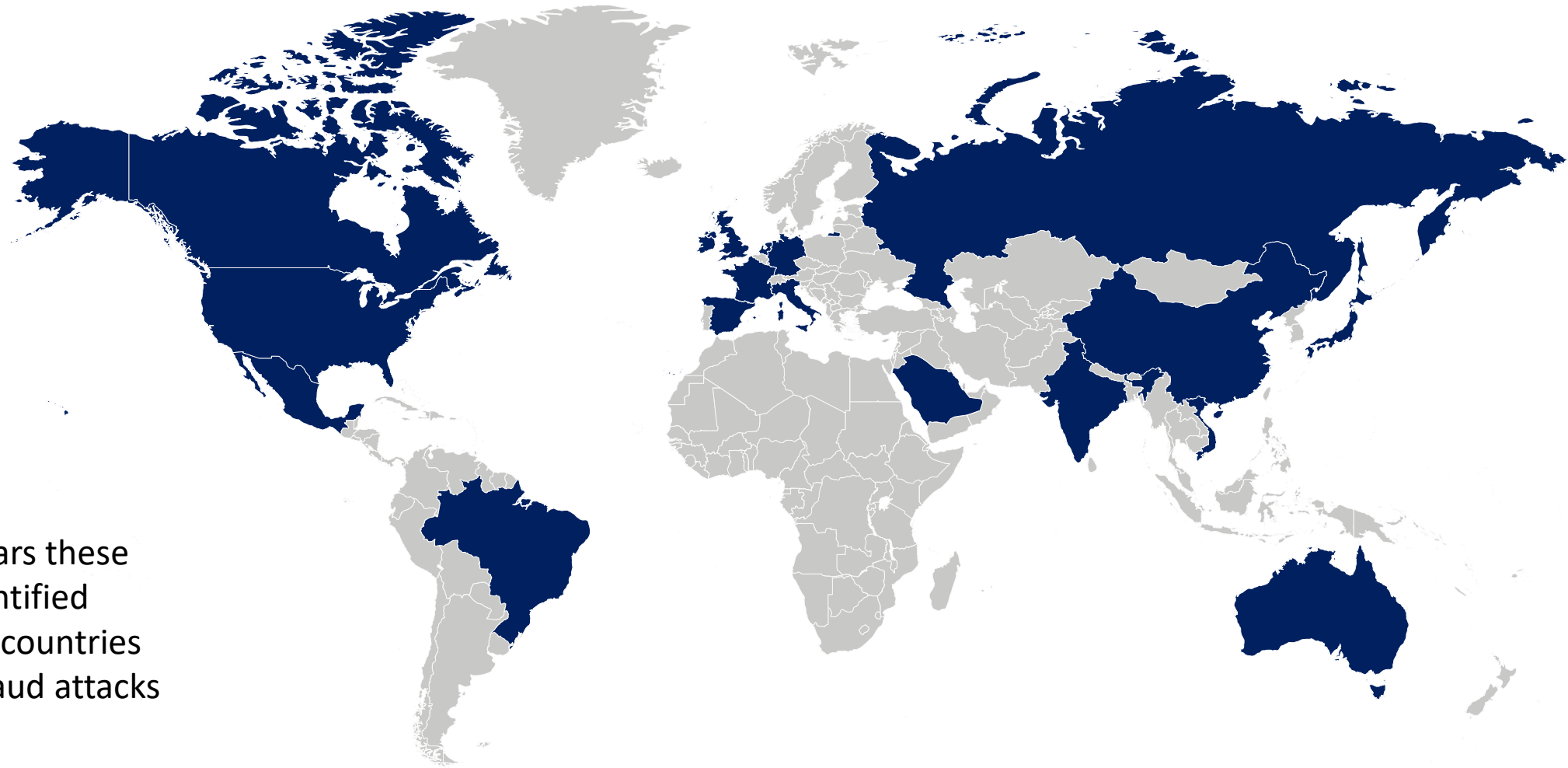
ATTACK VOLUME

1.6B

Growth YOY
+32% ▲

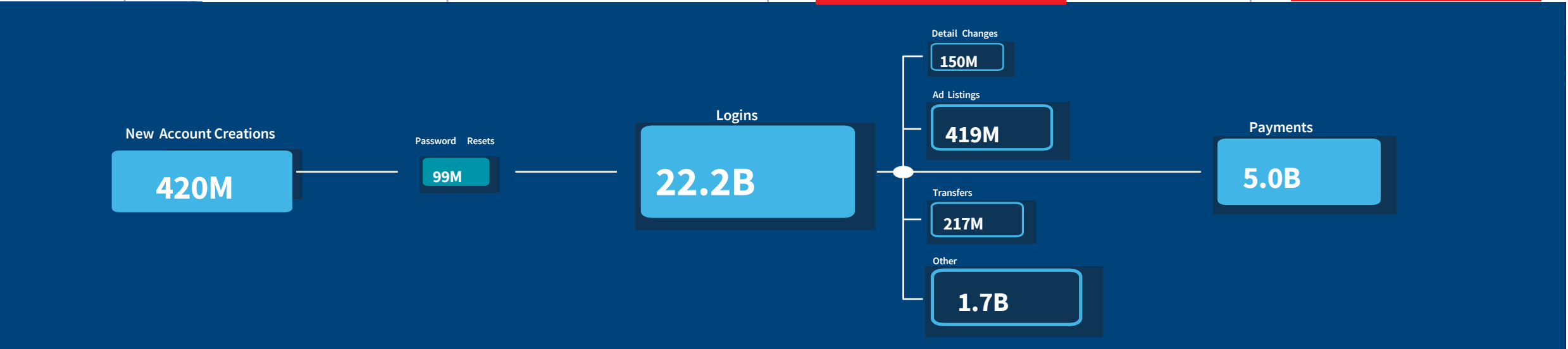
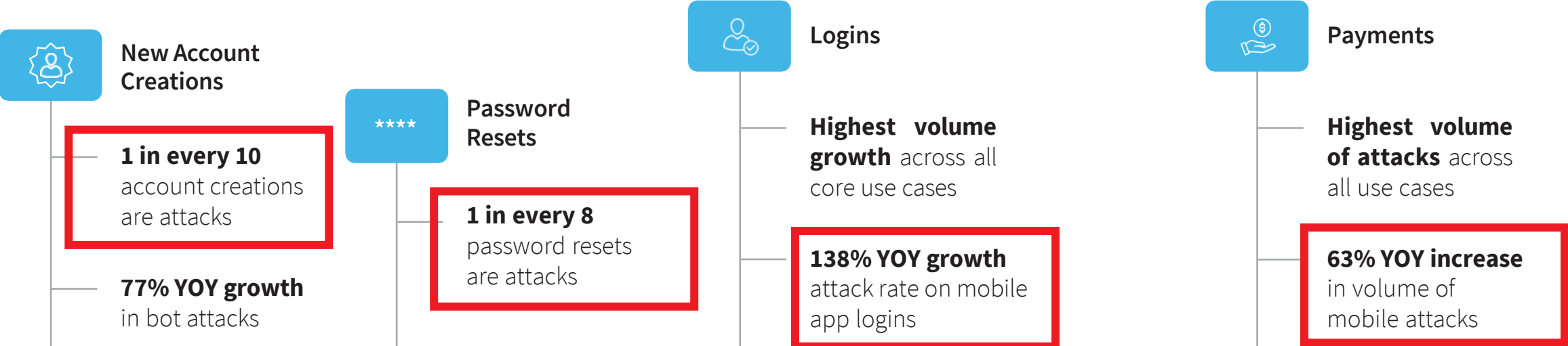
			Growth/Decline YOY
	Financial Services	890M	+10% ▲
	Ecommerce	275M	+32% ▲
	CMM	310M	+894% ▲

Top Attack Originators/Destinations 2015 - 2021



- Over the past several years these countries have been identified regulars in the top 10 of countries initiating or targets of fraud attacks

Issues Across the Customer Journey

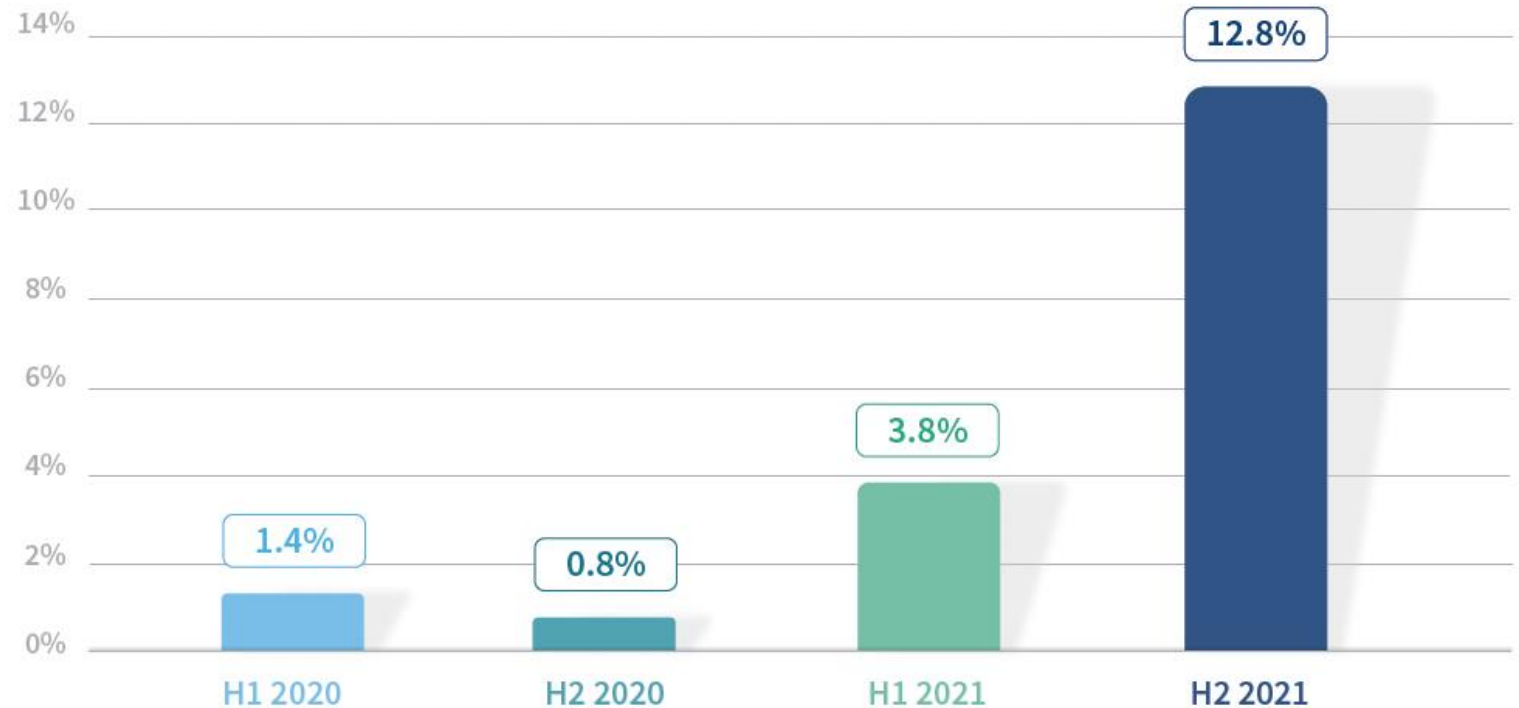


Password Reset – A New Focal Point For Fraud

The increase in attack rates is driven by:

- Digital user growth
- SCAMS
- Targeted Social Engineering
- Account Takeover

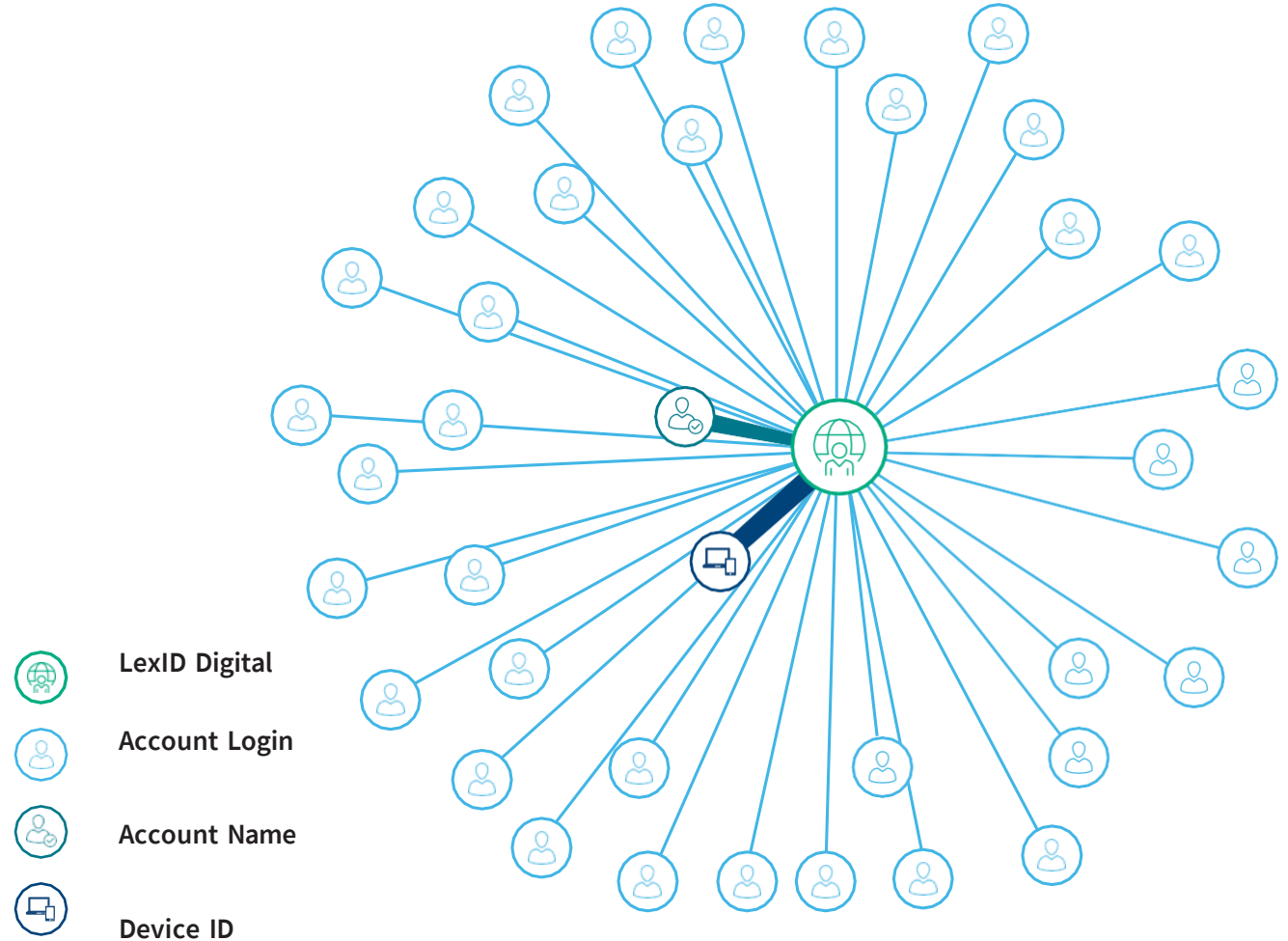
PASSWORD RESET ATTACK RATE



Password Reset – A New Focal Point For Fraud








A live example:

- One unique LexID® Digital entity indicates a single source of password reset abuse attacking multiple accounts.
- All events came via a hidden proxy, with the digital identity pretending to be in the U.S. while actually located within China.












Attack Risks Across Core Touchpoints









- **1 in 10** New account opening is attempted fraud
- Overall Login fraud attempts grew **24%**
- Payment mobile attack rate grew by **57%**

	 NEW ACCOUNT CREATIONS	 LOGINS	 PAYMENTS
ATTACK RATE			
 OVERALL	9.0%	0.5%	3.2%
 DESKTOP	13.3%	1.0%	3.7%
 MOBILE BROWSER	9.3%	0.6%	3.4%
 MOBILE APP	3.0%	0.3%	2.6%








Attack Risks Across Additional High-Risk Touchpoints

	 PASSWORD RESETS	 DETAIL CHANGES	 AD LISTINGS	 TRANSFERS	 OTHER
RISK TRENDS	Highest attack point for first time in the survey	To support interception of OTP & SMS detail changes for contact details growing	Increasing target of marketplaces where scams and immediate payment can be achieved for fraudster driving growth in this area	Transfers are still a target, but fraudsters are mixing their attack profiles across industries as organizations focused controls in this space	Other touchpoints such as beneficiary modification are still being targeted but use more traditional access as services are rolled out to APP
ATTACK RATE					
 OVERALL	12.8%	0.9%	0.5%	0.4%	1.0%
 DESKTOP	24.6%	0.9%	0.6%	0.9%	1.6%
 MOBILE BROWSER	1.7%	0.8%	1.0%	0.4%	1.0%
 MOBILE APP	3.1%	1.1%	0.5%	0.3%	0.6%

Industry Overview - Overview of Trends and Attack Patterns








INDUSTRY OVERVIEW	 ALL INDUSTRY SUMMARY	 FINANCIAL SERVICES	 ECOMMERCE	 COMMUNICATIONS, MOBILE AND MEDIA*	 GAMING AND GAMBLING*
RISK TRENDS	Attack rates increasing with. Financial services, gaming and gambling to the fore along side rapid growth in CMM	Attack rates up 24% YOY and 41% compared to h2 2020	SCA in Europe has lessened some scale attacks, with the shift focusing on marketplaces and G&G markets where instant revenue access is possible as a result of the attack	CMM has the highest attack rate by far and is a focus of both data gathering for social engineering and account takeover in order to support attacks against other verticals	Human initiated attack rates growing 146% on top of automated attacks in this space is creating pressure in the market
ATTACK RATE					
OVERALL 	1.1%	1.0%	1.4%	5.3%	1.5%
DESKTOP 	1.8%	1.5%	2.3%	3.9%	1.7%
MOBILE 	0.9%	0.8%	0.9%	6.0%	1.5%

Financial Services - Overview of Trends and Attack Patterns

FINANCIAL SERVICES OVERVIEW		 NEW ACCOUNT CREATIONS	 LOGINS	 PAYMENTS
RISK TRENDS		New account creations saw the highest growth in attacks, up 73% YOY as fraudsters target fast and easy onboarding for digital banking.	Account takeover attempts are generally tiny in comparison to the sheer volume of good customer interactions occurring daily. In spite of this, login attacks were up 48% YOY , with mobile app attacks up more than 200% .	Financial services payment attack rates are generally the highest across all the industries reported on. Attacks were up 25% YOY , with mobile app attacks up more than 400% .
ATTACK RATE				
OVERALL		7.0%	0.4%	4.5%
DESKTOP		11.5%	0.9%	4.1%
MOBILE BROWSER		7.8%	0.5%	4.5%
MOBILE APP		2.8%	0.3%	4.9%








Ecommerce - Overview of Trends and Attack Patterns

- EMEA has led the way with **61%** growth in payment transactions compared to the global average of **42%** growth.
- The accelerated shift to digital has driven merchants to commit to and fund their mobile app shopping experience.
- With increasingly easy methods for online payments and exclusive mobile app promotion deals, fraudsters are revising their attack vectors, with a noticeable rise in attacks on logins and new account creations via the mobile app,

ECOMMERCE OVERVIEW	 NEW ACCOUNT CREATIONS	 LOGINS	 PAYMENTS
RISK TRENDS	New account creation attacks continue to grow, up 29% YOY, with growth across desktop and mobile channels	Mobile app attacks at login have almost doubled globally, as fraudsters catch on to the fact that many merchants now have a designated mobile app.	Ecommerce payment attack rates continue to decline, down 18% YOY, driven by declines in Europe attributed to the ongoing roll-out of SCA in the payment journey due to PSD2 regulations.
ATTACK RATE			
 OVERALL	6.7%	1.0%	1.9%
 DESKTOP	12.7%	1.4%	3.4%
 MOBILE BROWSER	4.5%	0.7%	1.6%
 MOBILE APP	1.8%	0.5%	1.1%

Communications, Mobile and Media - Overview of Trends and Attack Patterns

- CMM has long been the fraudsters' preferred industry to test stolen credentials. Historically, the likes of social media and streaming platforms tend to have a different balance between user experience and fraud prevention as they may not be as heavily regulated as financial institutions.
- .The ability to create new accounts using stolen or synthetic identities can also provide access to valuable services or handsets that can be resold for profit.
- In this period a significant increase in automated bot attacks was observed, predominantly focused on credentials testing at login.

COMMUNICATIONS MOBILE AND MEDIA OVERVIEW	 NEW ACCOUNT CREATIONS	 LOGINS	 PAYMENTS
RISK TRENDS	Rates are however still higher than any other industry.	Login attack rate continues to be the highest overall across all industries and has held steady during this period.	CMM payment attack rates have declined by 31% YOY, driven by declines through the mobile channel.
ATTACK RATE			
 OVERALL	12.9%	1.3%	2.1%
 DESKTOP	16.8%	1.0%	3.7%
 MOBILE BROWSER	12.2%	0.9%	2.0%
 MOBILE APP	8.9%	5.1%	1.9%

Fraud Types Driving Attack Growth

Synthetic
Identity
Fraud

Account Take
Over (int)

Account Take
over (ext)

Credential
Testing

SCAMS

Authorised
Push Payment
Fraud

Targeted
Social
Engineering

Ad Listing
Fraud

The LNRS TCoF report – Shows the cost of fraud across channels highlighting the need for Omni channel Approach

Fraud Trends: As transactions become more omnichannel, so too is fraud. The average percent of fraud costs distributes fairly similarly across the in-person, online and mobile channels.

% Fraud Costs by Channel*

34%
In person

29%
Mobile

34%
Online store

11%
Call Centre / Telephone

4%
Other (kiosk, mail, other)

Fraudsters Leverage the Power of Networks to Facilitate Attacks



53,000+ Events

Were associated with the fraudulent digital identity



387,000+ Events

Recorded at other organizations in the Digital Identity Network that were associated with a digital identity that was involved in these original fraudulent events at source organizations



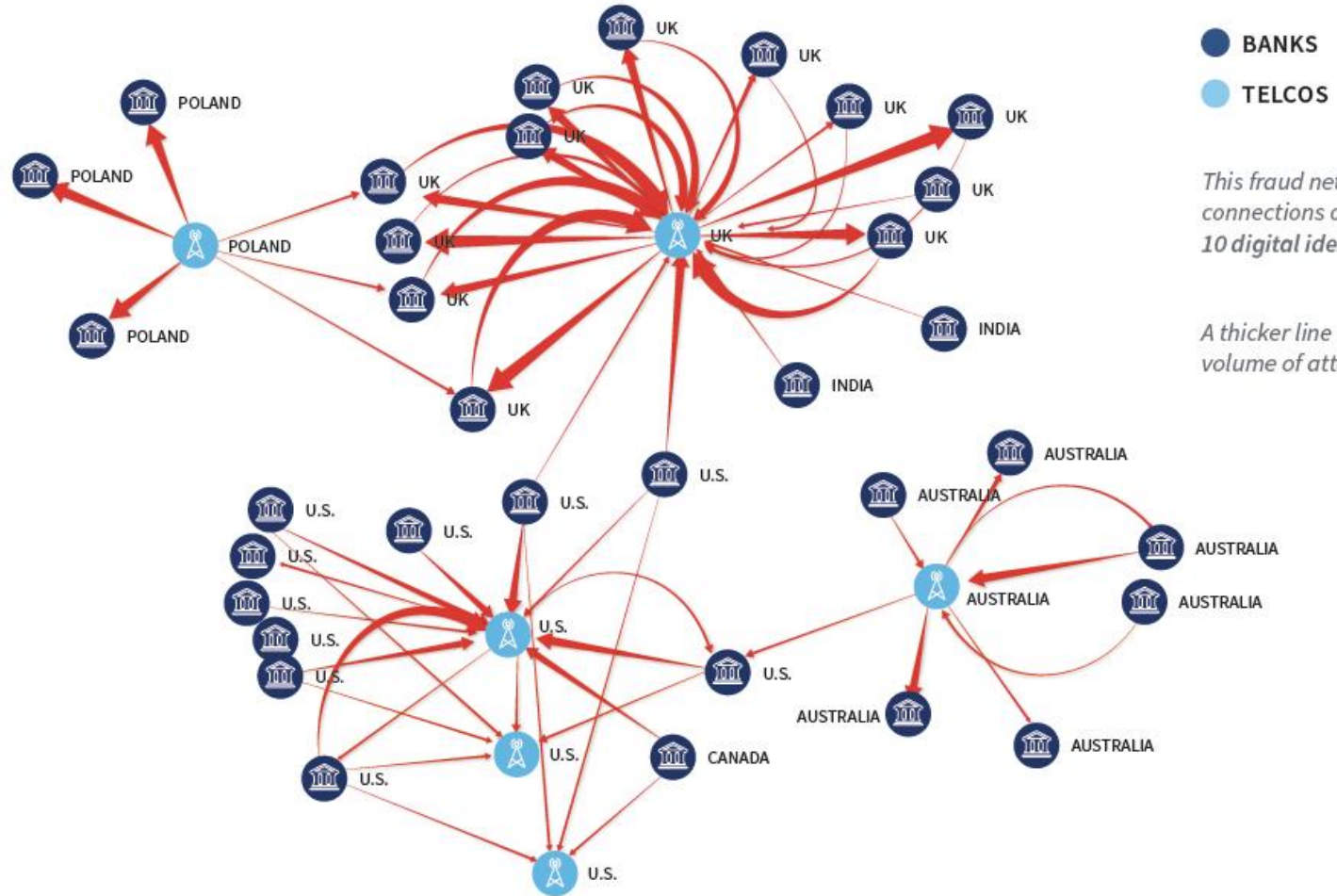
At least \$2.4M

In fraud blocked



At least \$10.3M

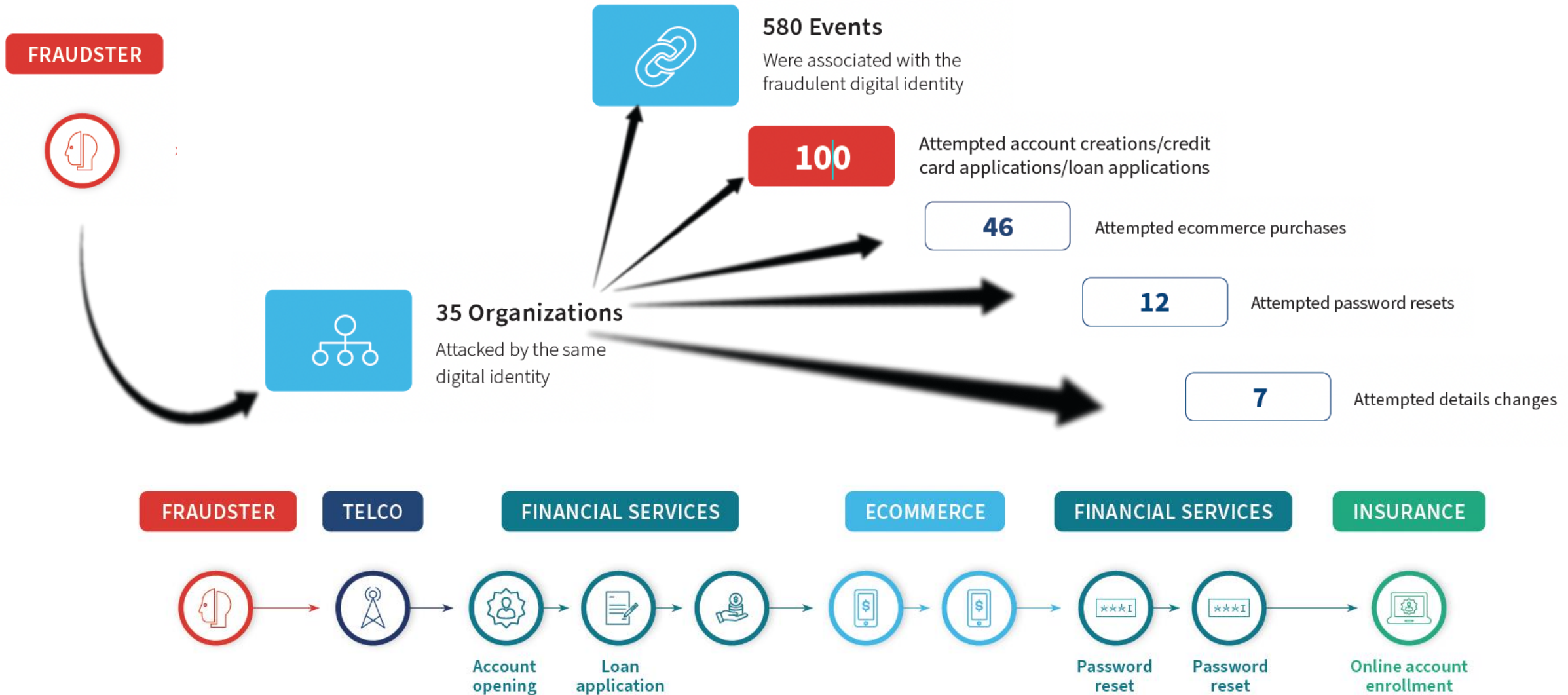
Was exposed to fraud across the entire network. Some of these transactions may have been blocked by organizations in the network who don't share fraud data.



This fraud network only shows connections of more than 10 digital identities.

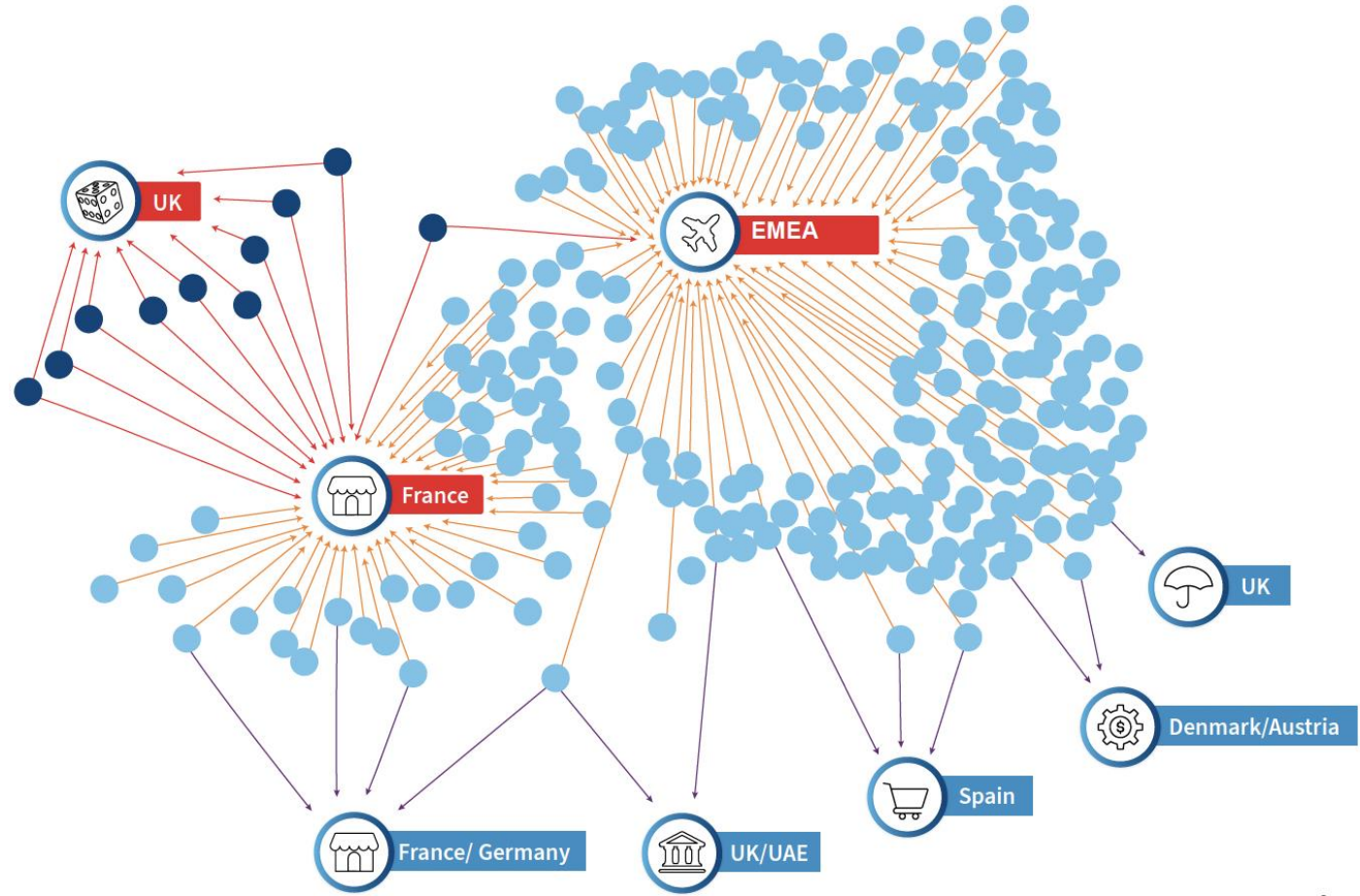
A thicker line denotes a higher volume of attacks.

The Life of a Prolific Individual Fraudster



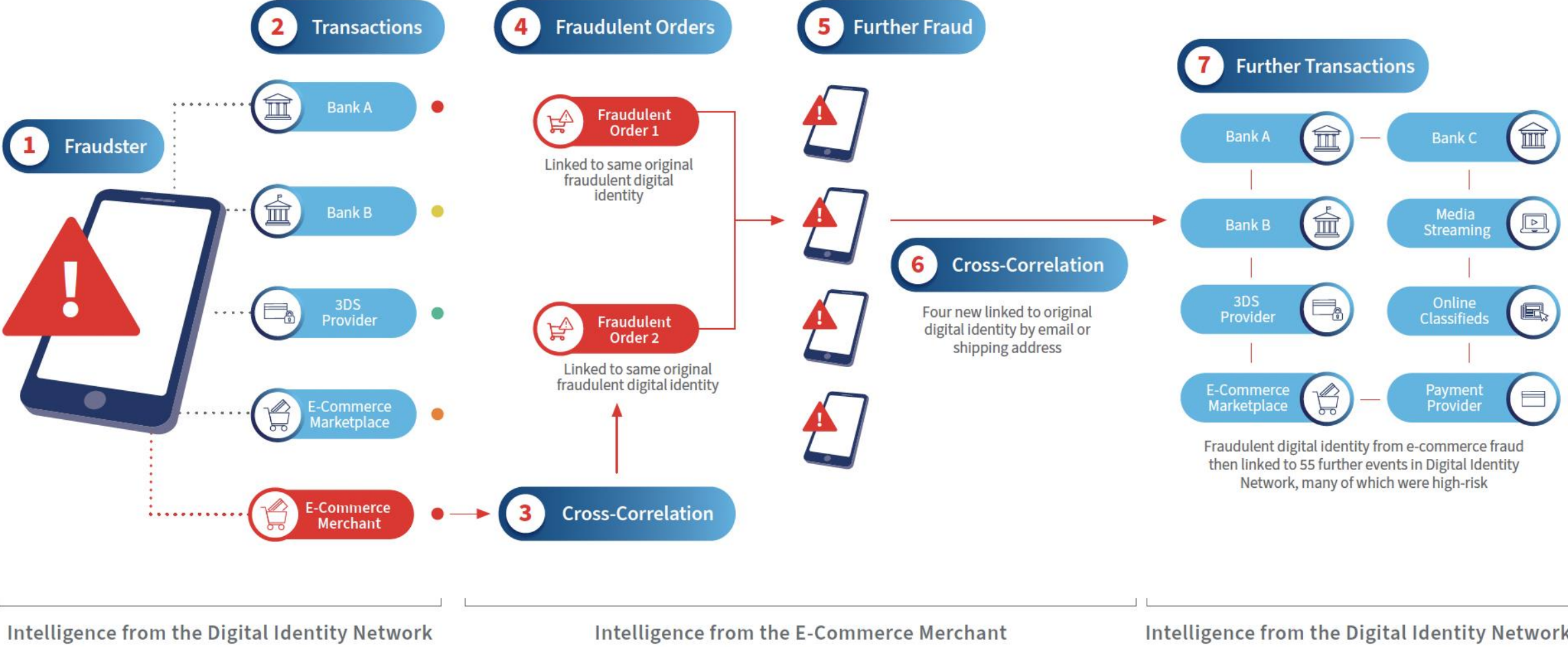
Showing the Links Across Verticals in Fraud Attacks using Emails

- ↑ Stolen email address used in attacks across organizations
- ↑ Stolen email address used in attack at one organization
- ↑ Email address used by genuine customer at other organizations



- GAMING AND GAMBLING OPERATOR
- AIRLINE
- RETAILER
- BANK
- MARKETPLACE
- FINTECH
- INSURANCE

Linking the Fraudster across the network



Download the full report from

<https://risk.lexisnexis.co.uk/insights-resources/research/cybercrime-report>

Thank You



Jason Lane-Sellers
Director, Fraud & Identity
LexisNexis Risk Solutions

Jason.lane-sellers@lexisnexisrisk.com

Joint Fraud Conference

