EMEA CYBERCRIME REPORT:

RISKS, TRENDS AND OPPORTUNITIES

July to December 2020

INTRODUCTION

FOREWORD

by Jason Lane-Sellers
Director, Market Planning EMEA Fraud and Identity
LexisNexis® Risk Solutions

2020 was an extraordinary year bringing significant change across the globe affecting the way we interact and operate at all levels. Unfortunately, over the past few years all of us are now becoming familiar with impacts of fraud and cybercrime. Regular news reports or alerts on fraud scams, data compromises or social engineering are common every week and impact people across all geographies. Personal data is now a valuable commodity and there are many bad actors out there eager to get their hands on it in order facilitate fraud schemes. In this particular year fraudsters have been opportunistic with their attacks against individuals and organizations, taking advantage of confusion and operational change caused by the global situation.

No organization or individual is safe from the unwanted attention of fraudsters – consumers, business, healthcare and government are all being targeted by criminals keen to exploit the changes that are being undertaken. Many organizations have had to accelerate digital transformation programs or offer new services or financial capabilities in a digital way for the first time in order to adapt to this global situation. This creates opportunity for criminal enterprise in exploiting weakness, lack of knowledge or understanding by consumers and organizations. The new vast array of technology available to us in enhancing our day to day lives and allowing business to connect with their users, also adds to this exposure to risk and provides criminals with many different ways to access their targets. As quickly as we are having to change our ways of interacting, it is essential for organizations to assess risk and manage the potential impact to both, themselves and the consumer.

Technology is also providing the answer, organizations are starting to arm themselves and protect customers against the threat of fraud and cybercrime This technology must enable customer experience to be a key part of the interaction and prevent risk without compromising the customer interaction. Organizations need to utilize the latest data and analytics tools in a way to enable prevention and management of fraud attacks and prevent impacts to consumers. In the new technological and digital world, organizations must fight fire with fire, utilizing the most accurate and current insights in order to effectively target fraud risk prevention.

INTRODUCTION

by Mélisande Mual
Managing Director, Publisher
The Paypers

The LexisNexis® Risk Solutions Cybercrime Report has always been one of our go-to sources on global development in the Fraud and Digital payments realm. We have been looking forward to the findings of the July-December 2020 edition. Last year consumers have moved dramatically toward online channels, digital payments have accelerated, and both merchants and financial services had to respond in turn. We could not wait to see how this seismic shift translated into the cybercrime domain.

Fraudsters follow the money and the opportunity. The risks attached to digital payments include fraudsters stealing bank account details, credit card credentials, social security numbers, and other personal information. Because of this, established merchants and financial services with long and proven track records serving consumers across multiple touchpoints tend to have multi-layered fraud defense systems and were pretty resilient to fraud.

However, those new to the digital channel are low-hanging fruit for fraudsters: on the merchant side these are the brick and mortar stores that were forced to open up a digital channel, and on the consumer side these are the age groups under 25 and above 75. Fraudsters have been actively targeting people who are new to electronic banking and they coerce these consumers into installing fraudulent applications or visit fraudulent websites masquerading as their real bank.

So what were the key findings for the EMEA region in the July-December 2020 edition of LexisNexis® Risk Solutions Cybercrime Report?

EMEA continues to experience low overall attack rates in comparison to the global averages, driven by a high volume of trusted mobile app transactions. The region experienced the biggest decline in the human initiated attack rate in comparison to other regions. However, several EMEA countries (Germany and the Netherlands) feature on the lists of largest contributors to both human-initiated and bot attacks, by volume.

Despite the lower overall attack rates in EMEA, the Cybercrime Report highlights two vicious attack vectors that require attention:

- Automated bot attacks to mass test stolen usernames and passwords against website login forms (credential stuffing)
- New Account Fraud, which is when fraudsters use these stolen identities or fake identities to open new (bank) accounts

As much as we all hope to be able to go back to a less digital and more normal social life, the seismic shift to digital is here to stay. Consumers have increasingly more choice in where to buy goods and services online. Competition is fierce and therefore there is a great need to offer good customers a frictionless customer journey across channels. Thus, being able to secure the entire customer journey (browsing – account creating – transacting – changing details in account) is the key to success.

We always look forward to the Cybercrime Report, and this one again has not disappointed: the report is filled with insights from all over the cybercrime world. I invite you to explore the report for yourself, and stay one step ahead of fraudsters once more.

2020: FULL YEAR REVIEW

A Global Summary of Transactions and Attacks January-December 2020

The forced consumer shift to digital channels drove rapid growth in trusted transactions, with an overall decline in attacks on businesses in LexisNexis® Digital Identity Network®. Growth economies contributed the largest growth in attack volumes. The analysis below represents the full year summary of transaction and attack patterns.

TRANSACTIONS PROCESSED

47.1B — 35.5B in 2019

Mobile transaction penetration:

67% — 65% in 2019

HUMAN-INITIATED ATTACKS

495M — 679M in 2019

Percentage of attacks coming from a mobile device:

56% — 55% in 2019

Largest attacker by volume:

United States

Largest growth in attacks from:

1. Guatemala
2. Bahrain
3. Zimbabwe

AUTOMATED BOT ATTACKS

2.1B — 2.0B in 2019

Largest attacker by volume:

United States

Largest growth in attacks from:

1. Isle of Man
2. United Arab Emirates
3. Nigeria

IDENTITY SPOOFING

Most prevalent attack vector

THE EMEA CYBERCRIME LANDSCAPE

EMEA TRANSACTION AND ATTACK PATTERNS

EMEA

TOP 5 ATTACKERS

1. UK
2. Germany
3. Saudi Arabia
4. Netherlands
5. Russia

TOP 5 ATTACK DESTINATIONS

1. U.S.
2. UK
3. Canada
4. Russia
5. Sweden

TRANSACTIONS

TRANSACTIONS PROCESSED

8.7B

Growth YOY
+23% ▲

TRANSACTIONS SPLIT BY CHANNEL

Desktop / Mobile

Mobile Browser / Mobile App

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

60M

Decline YOY
-54% ▼

AUTOMATED BOT ATTACK VOLUME

256M

Decline YOY
-6% ▼

ATTACKS SPLIT BY CHANNEL

Desktop / Mobile

percentage of attacks coming from mobile devices has **decreased YOY**

-13% ▼

LexisNexis® RISK SOLUTIONS

EMEA POSITION AGAINST GLOBAL FIGURES

EMEA

EMEA has Highest Penetration of Mobile App Transactions of any Global Region

GLOBAL EMEA

EMEA continues to experience low overall attack rates in comparison to the global averages, driven by a high volume of trusted mobile app transactions.

The region experienced the biggest decline in the human-initiated attack rate in comparison to other regions.

Despite this, however, several EMEA countries feature on the lists of largest contributors to both human-initiated and bot attacks, by volume.

Mike Nathan
Senior Director EMEA Solutions
Consulting, Fraud and Identity
LexisNexis® Risk Solutions

EXPERT COMMENTARY

CHANGING TIMES FOR DIGITAL CONSUMERS AND FRAUDSTERS

The July-December 2020 Cybercrime Report has provided some incredible insight into how digital users behavior has changed during the pandemic. We have witnessed an acceleration to digital first for commerce, banking, communications and leisure. Fraudsters follow the money; their behavior has also changed.

In EMEA, we notice that digital transactions are up 23% with a significantly higher adoption of companies' mobile applications. This increase to a more trusted channel (mobile is often more secure than web), has meant that in percentage terms fraud and high-risk events have come down. Mobile phone applications with the strength of physical biometrics, often means the only main point of vulnerability is the registration of the device. It is either all fraud or no fraud after that initial registration.

Fraudsters are changing their behavior, focusing more on automating their jobs, meaning that bots, scripts and credential testing volumes are more prevalent, whilst human-initiated attacks have decreased. Another interesting development is the eyes of EMEA fraudsters has swung to other mature global markets. This could be a consequence of the investment European companies are making in fraud and authentication solution to meet the incoming strong customer authentication (SCA) Payment Services Directive Two (PSD2) requirements. Through 2021/2022, we will be monitoring to see how regulation has impacted fraud, and it's success. We would expect to see a decline in the near future, as fraudsters adjust to the new landscape and seek easier targets. Once the fraudsters understand the new systems, in the longer term, it is likely they will focus their efforts on revenue streams closer to home.

> "Fraudsters follow the money; their behavior has also changed."

Rebekah Moody
Director, Fraud and Identity
LexisNexis® Risk Solutions

EXPERT COMMENTARY

THE PERVASIVE EFFECTS OF ORGANIZED, NETWORKED AND AUTOMATED FRAUD

While overall attack rates in EMEA are down year-on-year, this belies the fact that organized and networked fraud continues to play a pernicious and evolving role on digital commerce in the region.

Fraudsters are opportunists; looking for easy targets and new platforms to exploit. While some of these opportunities have likely taken the form of new lines of credit not seen in the Digital Identity Network, they have nevertheless continued to attack organizations across industries and country borders at scale.

This is clearly evident in new analysis that identified a huge payments fraud network operating across multiple eCommerce retails in EMEA. While consumers benefit from the close proximity and rich cultural diversity that the region offers, so too have fraudsters; operating across seven different countries and five different industries within the same overall fraud network. Lists of stolen identity data harvested from ever-present data breaches are the lifeblood of such networks.

These same lists are also mass tested by automated bots; again a key feature of the EMEA attack profile. The UK, Germany, Ireland and Netherlands all make the top ten list of largest originators of bot attacks by volume. Ireland and the Netherlands have also recorded significant growth in bot volume year-on-year. It may well be due to the full effects of such mass identity testing not yet being felt on organizations within EMEA. Validated credentials could, for example, form the linchpin to a cleverly engineered financial services scam downstream, making the fraud appear more credible to the victim by arming the fraudster with credentials that “only the bank would know”.

As EMEA works hard to recover from the effects of COVID-19, it will be incumbent on digital businesses to ensure they can protect consumers against the full spectrum of attacks, from mass identity testing to scams and account takeovers.

FRAUDSTERS LEVERAGE THE POWER OF NETWORKS TO FACILITATE ATTACKS

Hyperconnected Networks Continue to Target Multiple Industries and Organizations

The Digital Identity Network® continues to record a strong pattern of cross-organizational, cross-industry and even cross-regional fraud.

It is likely that each network comprises several groups of fraudsters using the same lists of stolen identity data, which are being exploited across regions and industries.

Devices associated with confirmed fraud events are likely tied to the same individual or fraud ring, given that hardware is not shared in the same way as stolen data.

The analysis in this report includes:

- The key links between devices and stolen identity data, including email addresses and telephone numbers.
- Transaction volumes that make up the fraudulent networks to illustrate the size and scale of fraudulent behavior.
- The assigning of monetary values to the entire fraud network based on known payment transaction amounts.

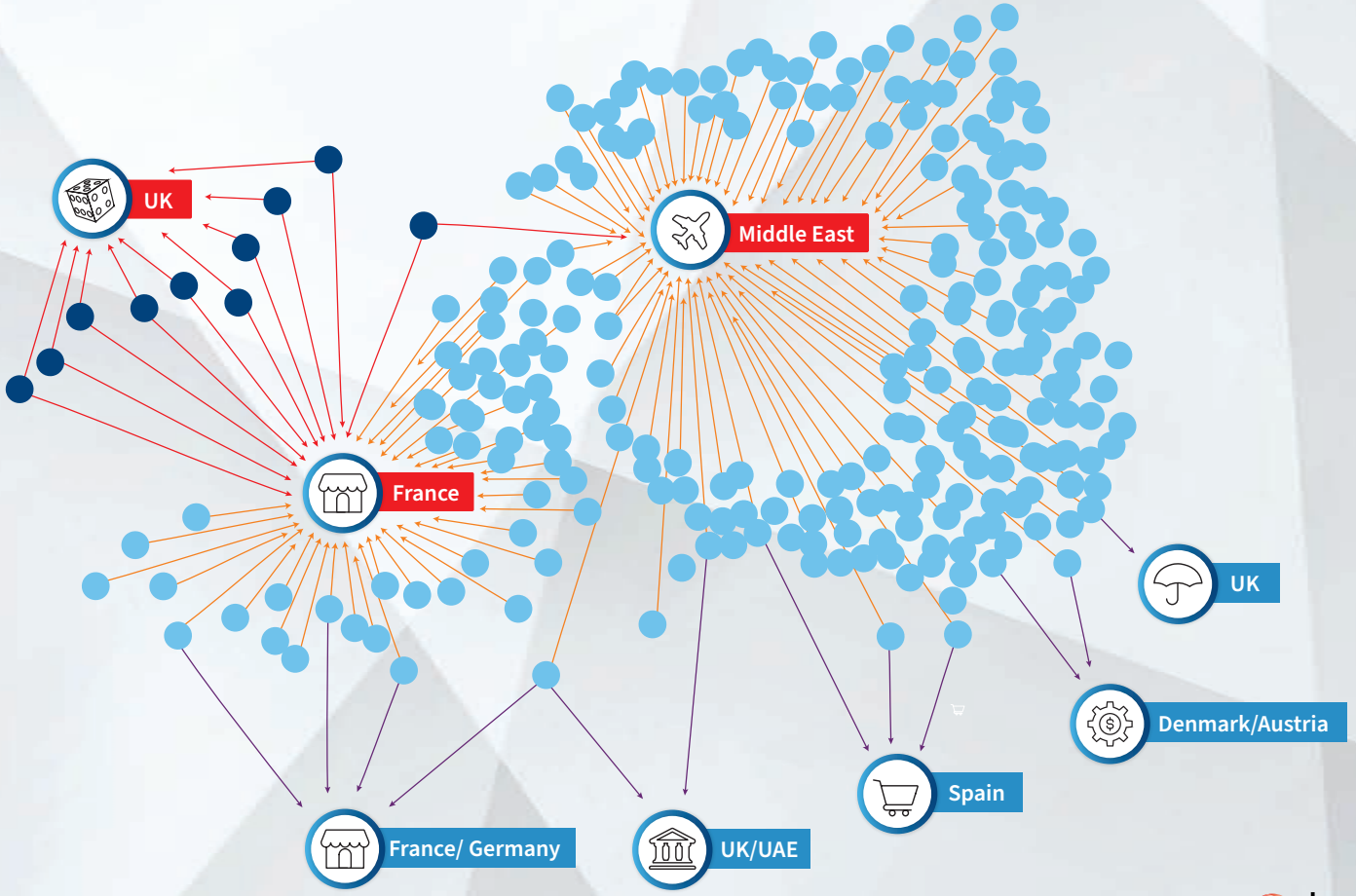
The Digital Identity Network allows organizations to share intelligence related to confirmed fraud events so that an entity that is marked as high-risk or fraudulent by one organization, can be reviewed by subsequent organizations before further transactions are processed.

USE OF STOLEN EMAIL ADDRESSES ACROSS ORGANIZATIONS HIGHLIGHTS THE IMPORTANCE OF ROBUST EMAIL RISK ASSESSMENT

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

LexisNexis® RISK SOLUTIONS

PAYMENTS FRAUD NETWORK RECORDED ACROSS MULTIPLE ECOMMERCE RETAILERS IN EMEA

The visualization on the following page shows a live fraud network targeting the eCommerce industry, operating across:

- Retailers, a marketplace and payment gateway in Germany
- A retailer and travel organization in France
- A retailer in the Netherlands
- A marketplace in Spain
- A loyalty program in United Arab Emirates
- A retailer in Latvia
- A retailer in Italy

As with the previous network, each arrow illustrates an entity associated with a confirmed fraud event at one organization crossing over to another organization in the Digital Identity Network. However, this fraud network sees a higher proliferation of fraudulent events connected through email addresses.

This shows groups of fraudsters working together to target multiple retailers, using shared stolen credentials.

NETWORK IN NUMBERS

2,000+

Events linked to confirmed fraud recorded at a source organization.

At least $750K

Fraud blocked.

3,000+

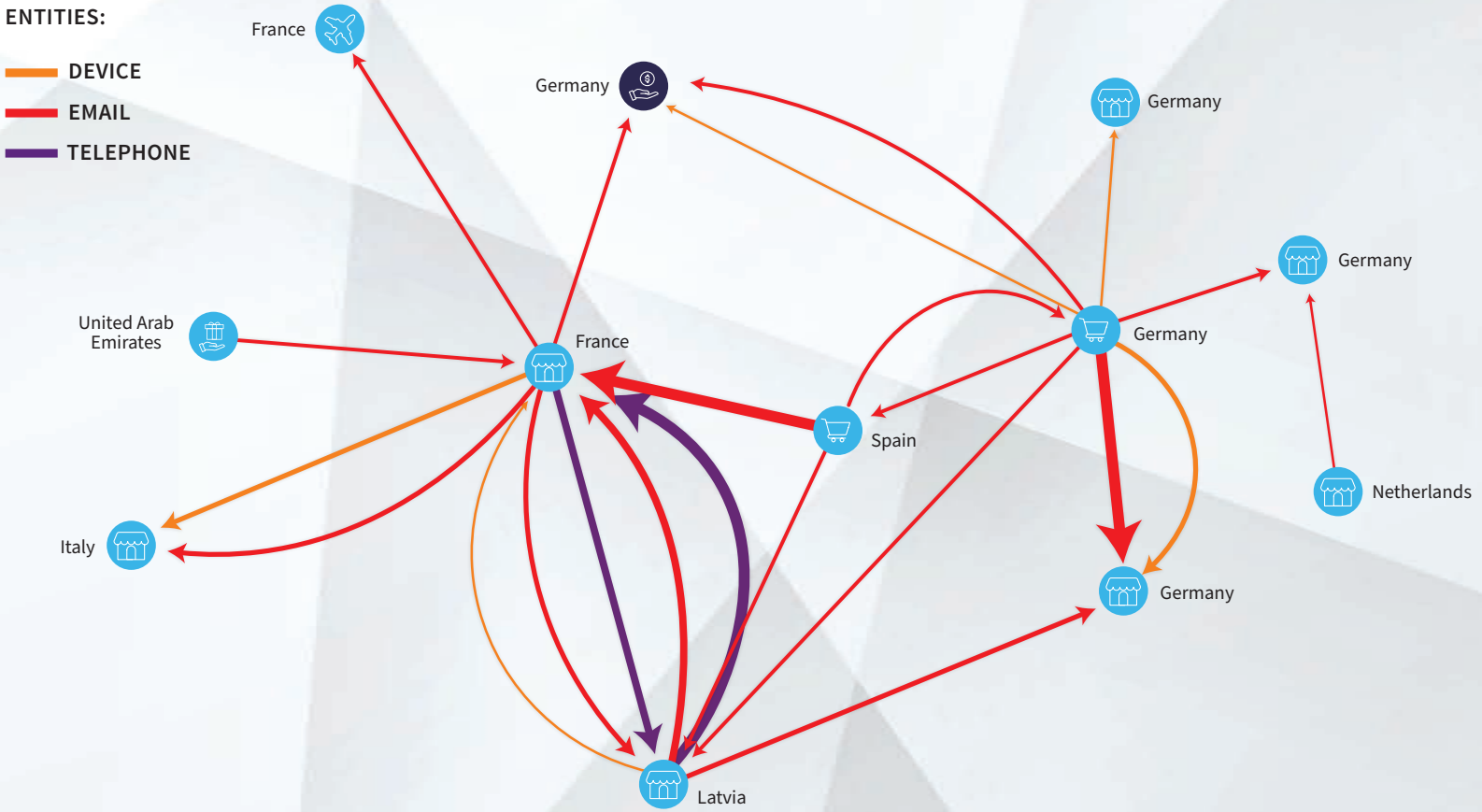
Events recorded at other organizations in the Digital Identity Network that were associated with either a device, email address and/or telephone number that was involved in these original fraudulent events at source organizations.

At least $250K

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

See next page for fraud network visualization

SHARED STOLEN CREDENTIALS USED BY GROUPS OF CYBERCRIMINALS FOR ACCOUNT TAKEOVER AND FRAUDULENT PAYMENTS



FINANCIAL SERVICES:

- PAYMENT GATEWAY

ECOMMERCE:

- MARKETPLACE
- LOYALTY PROGRAM
- RETAILER
- TRAVEL

This fraud network only shows connections of more than 10 entities. A thicker line denotes a higher volume of fraud.

LexisNexis® RISK SOLUTIONS

FRANCE SPOTLIGHT

FRANCE

TRANSACTIONS

TRANSACTION GROWTH YOY

+11% ▲

TRANSACTIONS SPLIT BY CHANNEL

Desktop / Mobile

Mobile Browser / Mobile App

ATTACKS

HUMAN-INITIATED DECLINE YOY

-73% ▼

AUTOMATED BOT DECLINE YOY

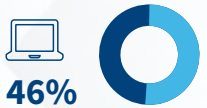
-60% ▼

TOP 5 ATTACK DESTINATIONS

1. France
2. U.S.
3. UK
4. Canada
5. Latvia

ATTACKS SPLIT BY CHANNEL

Desktop / Mobile



percentage of attacks coming from mobile devices has **decreased YOY**

-21% ▼

ATTACK RATES

- Overall **1.4%**
- Mobile Browser **1.7%**
- Desktop **1.3%**
- Mobile App **1.1%**

LexisNexis® RISK SOLUTIONS

Johanne Ulloa
Director Solutions Consulting
LexisNexis® Risk Solutions

EXPERT COMMENTARY

ATTEMPTS TO CIRCUMVENT MULTI-FACTOR AUTHENTICATION REMAIN A STRATEGIC ACTIVITY FOR FRAUDSTERS IN FRANCE

The most common method used to bypass two-factor authentication (2FA) is social engineering. This method is very effective, as it is the legitimate user who performs the authentication under the influence of the fraudster. The extremely low cost of this method (a simple phone call) as well as the almost absence of technical tools to implement it, make this method very attractive for fraudsters. If most of the time, it is the Short Message Service (SMS) authentication that is bypassed, we have observed a tendency to bypass other methods with advanced phishing tools such as EvilGinx. This tool is positioned as "man in the middle" and interacts with both the user and the website. It intercepts session cookies that are obtained by the victim after the authentication steps. The fraudster just has to replay these cookies for being authenticated on the victim account. It is therefore to be expected that this type of tool will be used more often, as many organizations do not yet have the solutions to correctly assess digital intelligence, which would nevertheless make it possible to limit the risks of 2FA bypass.

The industrialization of cyber criminals is not a new thing, fraudsters have a business approach and their objective is therefore to maximize profits which leads them to automate their attacks. Facilitated by massive data leaks, it gives them the raw material to carry out "credential testing" attacks. In France, we have also observed automated attacks that test the validity of stolen credit cards. These tests are made in order to reduce unsuccessful attempts on high-value goods. By minimizing their unsuccessful attempts with invalid cards, they maximize their chances of staying under the radar for longer.

For France, the volume of transactions increased significantly in the second half of the year (+22%). One would have expected the attack rate to increase as well, but instead, attacks have largely decreased (-53% for human-initiated attacks and -27% for automated attacks). This decrease is probably due to the effectiveness of the anti-fraud solutions offered by LexisNexis® Risk Solutions. Indeed, fraudsters always prefer the path of least resistance. If their usual targets become more difficult to reach, they turn to new ones that are more accessible.

GERMANY SPOTLIGHT

GERMANY

TRANSACTIONS

TRANSACTION GROWTH YOY

+96% ▲

TRANSACTIONS SPLIT BY CHANNEL

Desktop / Mobile

Mobile Browser / Mobile App

ATTACKS

HUMAN-INITIATED DECLINE YOY

-49% ▼

AUTOMATED BOT DECLINE YOY

-51% ▼

TOP 5 ATTACK DESTINATIONS

1. U.S.
2. UK
3. Canada
4. Sweden
5. Germany

ATTACKS SPLIT BY CHANNEL

Desktop / Mobile

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

+30% ▲

ATTACK RATES

- Overall **0.7%**
- Mobile Browser **1.3%**
- Desktop **0.6%**
- Mobile App **0.3%**

LexisNexis® RISK SOLUTIONS

Mathias Schollmeyer
Principal Solutions Consultant
LexisNexis® Risk Solutions

EXPERT COMMENTARY

THE LEXISNEXIS® DIGITAL IDENTITY NETWORK® DELIVERS TRUST FOR GERMANY'S GROWING DIGITAL WORLD

The COVID-19 pandemic has accelerated Germany's adoption of digital channels even more than in other countries. While still being a cash-first country, consumers were driven to online channels to do their shopping or banking due to branches being shut. While some industries took a huge hit, eCommerce benefited the most with reports of two digit growth across the industry.

Germany is lagging behind other countries in embracing mobile transacting, with still only 50% of traffic coming from a mobile device (compared to 69% globally). Fraudsters however have adopted more quickly with attacks originating from mobile devices representing 54% of all attacks. That is a year-on-year increase of 30%, outperforming legitimate consumers' transition. Digital first consumers and weak onboarding processes have enabled fraudsters to execute more targeted attacks, e.g., use social engineering to retrieve SMS 2nd factor authentication codes. The scammers tricking the victim into believing they are talking to a genuine staff member. The scammer had the victim's details already, gathered by a previous phishing attack or an undisclosed breach. The only missing piece was the SMS one-time password (OTP) for authorization. Another trend is attackers using the weaknesses in digital onboarding processes. While multi-factor authentication (MFA) is now more broadly accepted and enforced by regulations, the registration process is exploitable. With mobile authentication apps in particular, the attackers register their device with the consumer's details and evade these additional security measures.

While this is disconcerting, there are positive trends overall. Both, the human-initiated as well as the automated attacks have declined by roughly 50% compared to the previous year. The Digital Identity Network has seen an increase in transactions of almost 100% from Germany. The growth in transactions with a still relatively low attack rate means that consumers in Germany benefited from the Network's intelligence. Allowing merchants and services to trust a consumer's digital identity in near real-time to reduce fraud and enable an improved user experience. Consumers are being challenged less, they can be offered more payment options like buy-now-pay-later and can navigate through the checkout process without friction leading to an enhanced conversion rate.


CONCLUSION

PREDICTIONS FOR THE YEAR AHEAD: THE OPPORTUNITY FOR DIGITAL BUSINESSES

With change, huge opportunity often emerges. This opportunity, however, presents itself not just to forward-thinking digital businesses, but also to cybercriminals who can remain just ahead of the technology curve. As organizations continue to merge their digital and physical services, innovating to meet an increasingly diverse consumer base, fraud prevention strategies must keep pace with this evolution, transformation and growth. Without a robust, and layered approach, businesses are opening themselves up to new fraud risks. Fraudsters remain masters of disguise, continually searching out the weakest link under a cloak of legitimacy.

This weakest link may well be those new-to-digital customers who have come online during the pandemic. Younger adults and the older population have been shown to be the most susceptible to fraud attacks. Fraud prevention extends not only to detecting identity spoofing, automated bot attacks and account takeovers, but also to awareness, education and customer messaging that shows all customers how to better spot potential scams. It is likely that we will continue to see fraudsters preying on pandemic-related anxieties, offering investments that look too good to be true or products that are in hot demand online.

> "Without a robust, and layered approach, businesses are opening themselves up to new fraud risks."

PREDICTIONS FOR THE YEAR AHEAD: THE OPPORTUNITY FOR DIGITAL BUSINESSES (CONTINUED)

However, not only new customers must be protected. Trusted, existing customers may be inconvenienced with additional authentication steps as "back to normal" behavior is potentially flagged as unusual following the unprecedented change that took place in consumer behavior in 2020. How can organizations ensure that reliable fraud prevention does not mean unnecessary friction for good customers? Regulatory change and economic uncertainty will also merge with this evolving digital landscape.

Open banking platforms will become a key target for fraudsters looking to exploit customer data across accounts. PSD2 in Europe will see fraudsters looking for loopholes and exemptions in tighter fraud defenses.

Again, good customers may see a change to transaction acceptance rates with the new swath of authentication strategies that mandate two layers of strong customer authentication (SCA).

It is likely too that as economies respond to the impact of the pandemic, fraudsters will look to benefit from the downturn via increased mule recruitment, promising consumers fast money in return for use of their bank account to funnel proceeds of crime through global organizations.

eCommerce merchants will likely see a growth in first-party fraud as more consumers feel the economic pinch.

Market-leading innovation will continue apace to facilitate this complex set of opportunities and mitigate associated risks for global digital businesses. At its core, this should provide businesses with the ability to layer digital and physical identity and authentication solutions across an omni-channel customer journey.

DOWNLOAD THE FULL GLOBAL REPORT

The EMEA Cybercrime Report is a supplement to the LexisNexis® Risk Solutions Global Cybercrime Report, which is based on cybercrime attacks detected by the LexisNexis Digital Identity Network from July – December 2020. From global risks and industry opportunities, to analyzing the cybercrime landscape in a pandemic, download your free copy of the global cybercrime report today to learn how to tackle fraud and build trust with genuine customers.

LexisNexis
RISK SOLUTIONS

NXR14854-00-0321-EN-US