CYBERCRIME IN EMEA
2021 HIGHLIGHTS

The LexisNexis® Risk Solutions Cybercrime Report, January to June 2021

LexisNexis® RISK SOLUTIONS

EMEA TRANSACTION AND ATTACK PATTERNS

TOP 5 ATTACK ORIGINATIONS

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

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

Attacks out of EMEA are primarily targeted at companies and individuals based in the U.S.

TRANSACTIONS

TRANSACTIONS PROCESSED

EMEA
9.4B Growth YOY +19% ▲

GLOBAL
28.7B Growth YOY +28% ▲

ATTACKS

AUTOMATED BOT ATTACK VOLUME

EMEA Growth YOY
+13% ▲

Global Growth YOY
+41% ▲

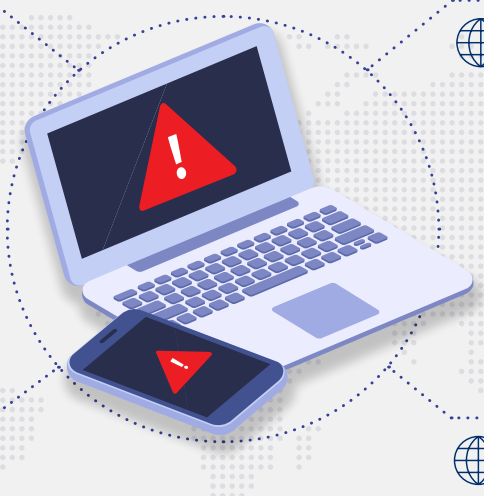
HUMAN-INITIATED ATTACK VOLUME

EMEA Decline YOY
-25% ▼

Global Decline YOY
-29% ▼

EMEA experiences lower overall attack rates with the global comparison as fraud tools are mature in particular markets and Strong Consumer Authentication becoming the norm in Europe. However, Africa and the Middle East particularly see a rise in scams.

	GLOBAL	EMEA
OVERALL ATTACK RATE	1.0%	0.6%
DESKTOP ATTACK RATE	1.4%	1.2%
MOBILE BROWSER ATTACK RATE	1.8%	1.4%
MOBILE APP ATTACK RATE	0.4%	0.1%



INDUSTRY OVERVIEW: TRENDS AND ATTACK PATTERNS IN EMEA

Customer experience suffers while fraud prevention increases across EMEA

While the rollout of PSD2 across Europe plays a big role in reducing fraud levels, it also leads to an increase in basket abandonment: 25% in average across the region.

Identity testing attacks in media organisations

Criminals have realised if they can access a digital online account, they can use the real data in a social engineering scam, such as payments details, address or even services last used.

FINANCIAL SERVICES	ECOMMERCE	MEDIA
0.4%	0.8%	2.5%

% of all transactions are attacks

Attack volume and attack rate are calculated using a subset of the total transaction volume, where outliers and unknown sessions are removed.

Scams have exploded in volume and complexity and are fast becoming the scourge of financial services and ecommerce merchants alike.

THE SCAM INTRODUCTION

Before making contact with a customer, the fraudster typically has already gathered data about the target from credential testing, exploiting security weaknesses on your devices or network and account access among other strategies. When in touch with the customer, they socially engineer them into believing they have a good opportunity to make money, or that their accounts have been compromised and their funds are at risk.

METHODOLOGY

Fraudsters play on a victim's worry, concern or sense of urgency, which can make it very hard to interrupt a payment transaction. A payment is made from the legitimate account holder as part of a fully authenticated online banking session. Alternatively, the customers complete an SCA check during a fraudster-initiated Card Not Present purchase.

ATTACK

Real-time payments protocols mean that money can leave a victim's account immediately and can be very hard to trace or recover, particularly if the money has been split and passed through a series of mule accounts.

LexisNexis Fraud and Identity solutions establish a true identity by leveraging network intelligence, industry-trusted global coverage and intellectual property to **enable your business to confidently differentiate between a trusted customer and a cyber threat in milliseconds, while maintaining a seamless customer experience.**

Click here to view the complete findings from our latest **Cybercrime Report**