LexisNexis®
RISK SOLUTIONS

ANSWER THE TOP 5 CYBERCRIME CHALLENGES

PREVENT CYBERCRIME UP-FRONT WITH THE ADVANTAGE OF A DYNAMIC, NEAR REAL-TIME VIEW OF IDENTITY

TABLE OF CONTENTS

WELL-NETWORKED FRAUD RINGS DECISIVELY TARGET DIGITAL ECOSYSTEM VULNERABILITIES

Bot volume shows a 42% increase in North American markets.[1] Defined consumer shifts to digital channels are being closely mirrored and capitalized on by cybercriminals. Organized networks continue to industrialize fraud and leverage specific threat vectors to successfully target key customer interaction points. These rising levels of fraud volatility demand a near real-time response that reflects current user behaviors.

The changing dynamics of customer interactions create a hospitable climate for cybercrime. Businesses are challenged to balance convenience and safety at every customer touchpoint across an omni-channel ecosystem. The line between trusted customers and cybercriminals continues to blur as breached identity information multiplies and synthetic identity fraud gains strength. Understanding and capturing changing interaction patterns in near real-time is integral to confident customer recognition.

Our eBook delivers latest insights from the LexisNexis® Risk Solutions Cybercrime Report. Inside you will learn the best tactics to answer the top 5 cybercrime challenges. Find out why dynamic interaction intelligence reinforces fraud defenses and helps reduce friction for trusted customers.

[1] *LexisNexis® Risk Solutions Cybercrime Report, January-June 2021*

NEW ACCOUNT CREATION REMAINS A HIGHLY VULNERABLE CUSTOMER TOUCHPOINT

CHALLENGE:

New account creations continue to be attacked at a higher rate than any other transaction type in the customer journey. Around 1 in every 11 new account creation transactions tracked by the LexisNexis® Digital Identity Network® is an attempted attack.

SOLUTION:

As cybercriminals use stolen, compromised or synthetic identities to create new accounts, identity trust plays an integral role in a strong cybercrime defense. The ability to rapidly recognize good, trusted customers and quickly determine the validity of the customer credentials contributes to a seamless and secure account opening experience. **LexisNexis® ThreatMetrix®** establishes a true digital 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.

Combining digital and physical identity capabilities gives organizations an extensive view of the consumer so they can quickly pivot against new threats and create a better customer experience.

PREVENTING ACCOUNT LOGIN ATTACKS HELPS PRIORITIZE TRUSTED CUSTOMER INTERACTIONS

CHALLENGE:

Our Cybercrime Report showed automated bot attacks attempting account takeovers at login have grown 52% year-over-year (YOY). Account takeovers are also shifting further towards the mobile channel, with 44% of attacks now targeting mobile, compared to 36% in 2020. Proactively avoiding account login attacks is critical to protecting trusted customers and preventing costly chargebacks and losses.

SOLUTION:

Account takeover via a fraudulent login creates an easy avenue for cybercriminals to monetize compromised identity credentials and stolen credit cards. Reliable and robust authentication can reinforce account login defenses. Confidently recognizing behavior patterns and fully understanding the **digital DNA** of trusted users helps isolate and identify deviations that may signal fraud. **LexisNexis® ThreatMetrix®** with **behavioral biometrics** leverages proven machine learning threat intelligence to expose inherent user behaviors without compromising privacy, or introducing unnecessary friction to customer interactions. When there are scenarios for step up authentication, it is important to provide risk appropriate alternatives that meet customer experience expectations.

PAYMENT TRANSACTIONS ARE A HIGH-RISK ENTRY POINT FOR CYBERCRIME

CHALLENGE:

At 4.0 billion, the volume of payment transactions is continuing an upward trajectory in 2021 as the shift to digital commerce becomes more permanent. Our study shows a higher volume of attempted attacks on payment transactions than any other customer touchpoint. Payments also show 18% YOY growth in automated bot attack volume.

No industry is immune from risk entering the payments touchpoint. Mobile browser payment transactions experienced an attack rate of 2.7%. Similarly, the mobile app attack rate on ecommerce payment transactions is 2.0% and financial services payment transactions recorded an overall attack rate of 2.9%.

SOLUTION:

Cybercriminals are taking the opportunity created by digital payments to cash out and monetize stolen credentials. A strong payments defense rooted in identity trust is essential as consumers rely on digital payments throughout omni-channel ecosystems. **LexisNexis® ThreatMetrix®** with **behavioral biometrics** strengthens payment fraud prevention by combining digital identity intelligence and global transaction insights in near real-time. Improve transaction security and refine personalization with direct risk intelligence that helps your business confidently differentiate between a trusted customer and a cyber threat.

HYPERCONNECTED FRAUD NETWORKS WREAK HAVOC ON STATIC APPROACHES TO FRAUD PREVENTION

CHALLENGE:

The Digital Identity Network® continues to record a strong pattern of cross-organizational, cross-industry and even cross-regional fraud. Hyperconnected networks continue to exploit the same lists of stolen identity data across multiple regions and industries. Networked fraud remains a highly nuanced threat that easily evades traditional fraud prevention tools like static point solutions.

SOLUTION:

A dynamic, multi-layered fraud prevention strategy is pivotal to protecting your business in a rapidly evolving cybercrime environment. The **Digital Identity Network®** connects businesses to a shared view of fraud that includes intelligence relating to online behavior, transaction trust and risk, global block lists, allow lists and watchlists, as well as targeted industry models. By leveraging a collaborative approach, an entity confirmed as high-risk by one organization can be blocked by subsequent organizations before further transactions are processed, improving fraud prevention and adding a layer of protection against networked attacks.

AUTOMATED BOT ATTACKS PERSIST AS A PREVALENT ATTACK VECTOR

CHALLENGE:

Our study shows automated bot attacks continue to be widespread, recorded across global regions and attacking a wide variety of industries and use cases to mass test identity credentials. Automated bot attack volume from January-July 2021 was 1.2B with both the media industries (up 174%) and financial services industry (up 28%) experiencing significant growth in automated bot volume. All four global regions are represented on the top 10 list of the largest originators of automated bot attacks by volume, with the United States, the United Kingdom and Japan representing the top three originators. Brazil and Mexico now both appear in this top ten list, further establishing the LATAM region as a top attack originator.

SOLUTION:

Bot attacks represent a cheap, quick and effective method of initial attack that enables identity testing at scale, providing the opportunity for cybercriminals to validate and rapidly monetize stolen credentials. Proactively detecting bot attacks without disrupting legitimate customer interactions or adding friction to key customer touchpoints takes a delicate balance. **LexisNexis® ThreatMetrix®** with **behavioral biometrics** refines visibility into transaction risk so your business can seamlessly distinguish between a trusted customer and an automated bot. By leveraging a unified picture of identity informed by network intelligence and targeted visibility into risk signals that indicate bots and aggregators, our solutions help you confidently accelerate interactions with trusted customers and achieve near real-time detection of automated bot attacks.

INFORM IMMEDIATE IDENTITY TRUST AND RISK DECISIONS WITH DYNAMIC INTERACTION INTELLIGENCE

Trusted customers won't compromise on an efficient, secure and effortless interaction—every time. Near real-time visibility into customer behaviors and interaction patterns helps businesses balance high customer expectations with fortified security across omni-channel ecosystems. Achieving—and consistently delivering—a customer journey that centers on convenience and safety creates competitive advantage by crystalizing customer affinity.

Our fraud and identity solutions enable businesses to directly determine identity trust so they can proactively detect fraud up-front. Our integrated tools combine a multi-layered view of identity with dynamic interaction insights and cross-industry fraud intelligence to empower near real-time responses to high-velocity cybercrime challenges on any channel. Prioritize personalized, more secure transactions for trusted customers while detecting and preventing cybercrime threats with the power of Identity Trust.

FOR MORE INFORMATION VISIT:

risk.lexisnexis.com/CybercrimeInsights

LexisNexis®
RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products. LexisNexis Risk Solutions does not warrant this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis Risk Solutions.

NXR15159-00-1021-EN-US

For more information, please visit risk.lexisnexis.com, and relx.com