LexisNexis®
RISK SOLUTIONS

TOP 5 WAYS TO FIGHT CYBERCRIME

OUTSMART CYBERCRIMINALS WHILE DELIVERING OPTIMAL, OMNI-CHANNEL CUSTOMER EXPERIENCES

TABLE OF CONTENTS

INTRODUCTION 03

CYBERCRIME CHALLENGES:

01 New Account Creation Remains a Highly Vulnerable Customer Touchpoint 04

02 Preventing Account Login Attacks Helps Prioritize Trusted Customer Interactions 05

03 Payment Transactions are a High-Risk Entry Point for Cybercrime 06

04 Hyperconnected Fraud Networks Wreak Havoc on Static Approaches to Fraud 07

05 Automated Bot Attacks Persist as a Prevalent Attack Vector 08

CONCLUSION 09

HYBRID CUSTOMER INTERACTIONS CREATE A HOSPITABLE CLIMATE FOR CYBERCRIME

In every industry, organizations continue to merge their digital and physical services within an omni-channel ecosystem. Routes to purchase are increasingly converging with in-store experiences being replaced by, or combined with, digital offerings. Digital payment solutions have also rapidly diversified, multiplying the number of routes for consumers to transact.

The changing dynamics around customer interactions create a hospitable climate for cybercrime to flourish. Well-networked cybercriminals are adept at leveraging specific threat vectors to relentlessly target key points across the customer journey. How can you best defend your business as cybercriminals capitalize on the acceleration of digital transformation?

Our eBook leverages the latest insights from the LexisNexis® Risk Solutions Cybercrime Report, July-December 2020, to detail the top 5 ways to fight cybercrime. Find out the best tactics to outsmart cybercriminals while delivering optimal, omni-channel customer experiences.

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 10 new account creation attempts 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 a holistic 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 9% growth in mobile login attacks year-over-year. Compounding this trend is the prevalence of identity spoofing which was seen in 5% of all global transactions. 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 3.7 billion, the volume of payment transactions has grown significantly in the past year as the shift to digital commerce becomes more permanent and pronounced. Our study shows a higher volume of attempted attacks on payment transactions than any other customer touchpoint. Mobile browser payment transactions experienced an attack rate of 3.4%. Similarly, the mobile app attack rate on eCommerce payment transactions is 2.7% and financial services payment transactions recorded an overall attack rate of 3.6%. No industry has immunity from this ubiquitous threat vector.

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 immediate 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. Our study shows organizations within the LexisNexis® Digital Identity Network® processed 24.6B transactions but experienced a 58% year-over-year decline in human-initiated attacks. 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 July-December 2020 was 1.2B with both the eCommerce (up 32%) and media industries (up 10%) experiencing 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 Canada representing the top three originators.

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.

PREVENT CYBERCRIME AND PROTECT AN INVALUABLE ASSET: CUSTOMER AFFINITY

The complex and constantly changing cybercrime climate challenges your business to balance interaction speeds with fortified security and a seamless experience at every point of the customer journey. Your trusted customers won't compromise on an efficient, secure and effortless interaction— every time. Consistently delivering optimal, omni-channel customer experiences defines competitive advantage in a crowded digital marketplace.

Building your cybercrime strategy on the foundation of a unified, risk-based identity view enables your business to deliver personalized, more secure transactions for trusted customers while accurately detecting and preventing cybercrime threats. Our solutions deliver a quickly configurable, near real-time and complete view of identity so your business can immediately refine fraud defenses to proactively respond to high-velocity cybercrime challenges on any channel. Fully capitalize on the opportunities of a well-connected omni-channel ecosystem by starting with the confidence 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 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.

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