LexisNexis®
RISK SOLUTIONS

Online Gaming Fraud in North America

The gaming and gambling industry faces threats at every stage of the customer journey. Fraudsters show no signs of abating.

We spoke to business leaders in the region to understand which types of fraud are doing the most damage and how they plan to fight back.

LexisNexis® RISK SOLUTIONS

Contents

Fraud and Identity Industry Pulse: Online Gaming in North America

Online gaming is a fast-evolving, highly competitive marketplace where new and existing platforms must use every tool at their disposal to attract and retain customers.

But tactics such as increasing promotional incentives and reducing friction leave the door wide open to fraud.

In this North American edition of our online gaming industry pulse survey, we share the challenges and preferred mitigation strategies of fraud and identity professionals in the region.

Key Takeaways

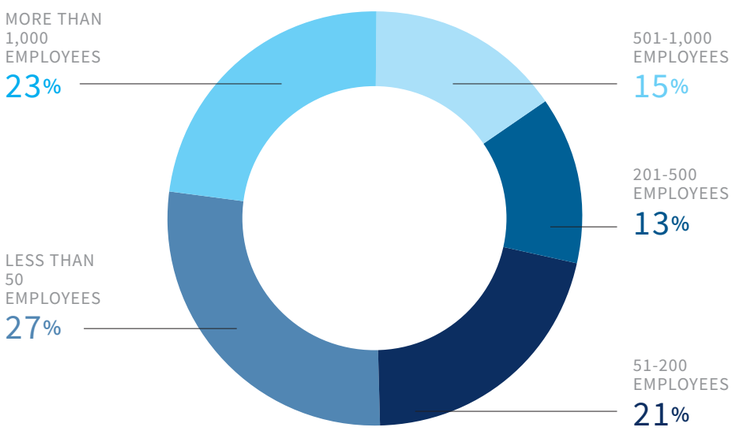
- Bonus abuse holds the house to ransom in North America. 78% of respondents aren't seeing fraud let up.
- Gaming fraud professionals stack their chips on multiple intelligence sets to fight back, leveraging manual monitoring, document verification and device fingerprinting as their top lines of defense.
- Improving customer UX and loyalty, plus improving fraud management, top North American respondents' 2026 wish list.

Taking the pulse of online gaming fraud

LexisNexis® Risk Solutions collaborated with SIS to conduct a survey of 993 decision-makers across the online gaming industry; only North American responses are analyzed here. Respondents included final decision-makers, decision influencers and those who evaluate customer-facing security, fraud detection and/or ID verification solutions. As percentages are rounded to whole numbers, some charts don't add to 100%. Ranked charts refer to weighted averages.

COMPANY SIZE

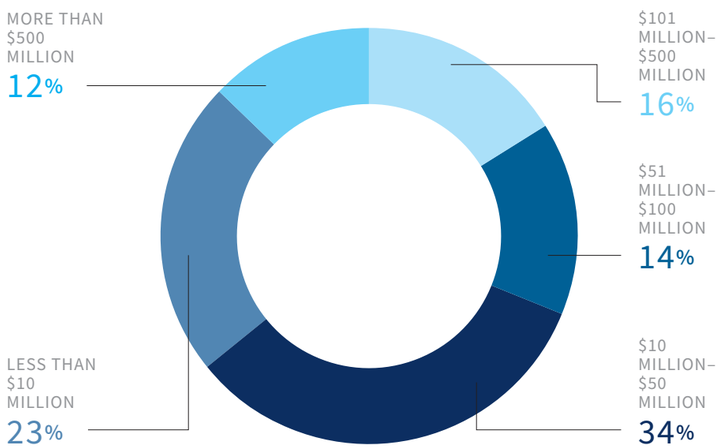
More than a quarter of respondents from North America worked at organizations with fewer than 50 employees, a fifth at companies with 51 to 200 employees and half at larger companies.



WHAT IS THE SIZE OF YOUR ORGANIZATION IN TERMS OF THE NUMBER OF EMPLOYEES? (NUMBERS DO NOT ADD TO 100% DUE TO ROUNDING.)

COMPANY REVENUE

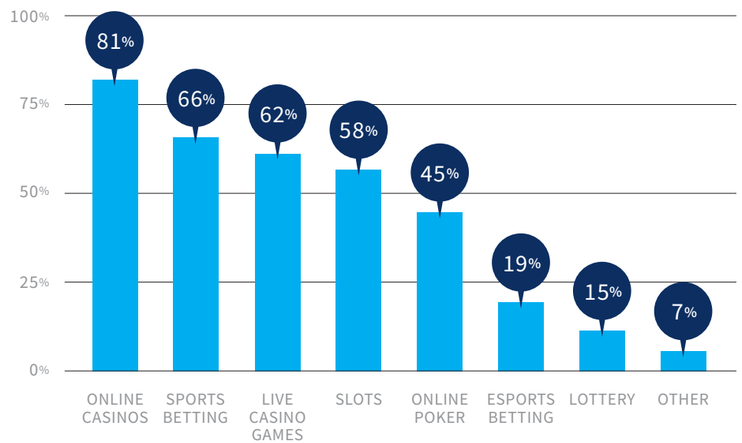
About a quarter (23%) of respondents were from companies with less than $10 million in annual revenue, 34% were from businesses with $10 to $50 million and 42% were from companies with revenue above $50 million.



WHAT IS YOUR ORGANIZATION'S ANNUAL REVENUE? (AMONG RESPONDENTS WHO SUPPLIED A VALUE; NUMBERS DO NOT ADD TO 100% DUE TO ROUNDING.)

PLATFORM OFFERINGS

81% of respondents' platforms offer online casinos, and about two-thirds provide sports betting (66%) and live casino games (62%). Smaller numbers of respondents' platforms offer online poker, slots and lotteries.



WHICH TYPES OF E-GAMING AND GAMBLING SERVICES DOES YOUR COMPANY OFFER?

Which type of fraud is impacting North American gaming operators the most?

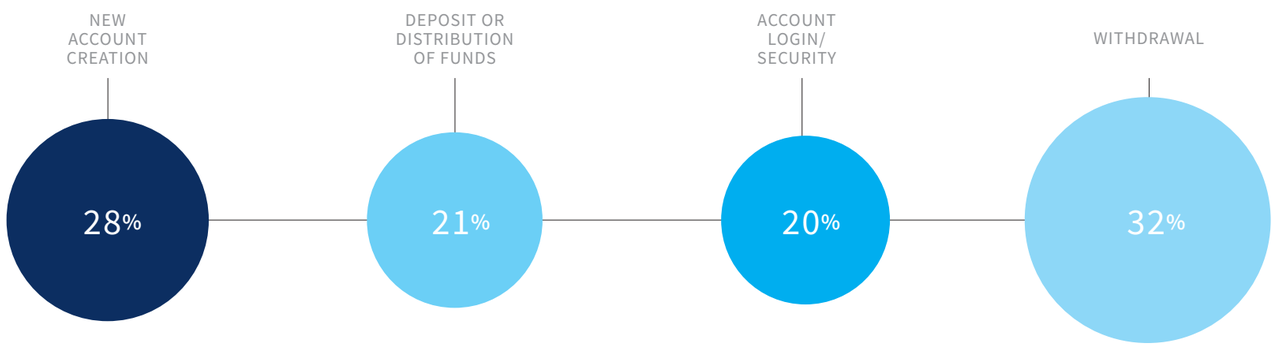
The most prevalent: bonus abuse

The increasing ease in obtaining new phone and email addresses is one of the many reasons behind this fraud category surge.

WHAT TYPES OF FRAUD AND/OR COMPLIANCE RISKS ARE IMPACTING YOUR ORGANIZATION THE MOST? (PERCENTAGE THAT LISTED EACH IN THEIR TOP THREE.)

Customer journey fraud hotspots: account creation and withdrawal

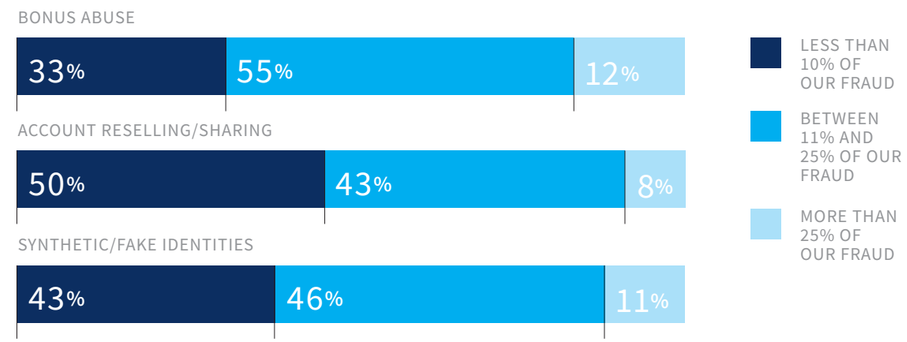
The beginning and ending of customer journeys are the most perilous for gaming companies. Respondents report that around 60% of fraud occurs in either the new account creation or the withdrawal phase of customer engagement. This trend is similar outside North America, demonstrating a global appetite for effective fraud prevention solutions at every stage of the customer journey.



APPROXIMATELY HOW MUCH OF YOUR ORGANIZATION'S FRAUD LOSSES WOULD YOU ATTRIBUTE TO EACH OF THE FOLLOWING CUSTOMER-JOURNEY STAGES? (COLLATED AND AVERAGED RESULTS. NUMBERS DO NOT ADD TO 100% DUE TO ROUNDING.)

The most negative impact on the bottom line: bonus abuse

It is perhaps unsurprising, given bonus abuse is the most prevalent type of fraud, that 12% of businesses attributed more than a quarter of their losses to this fraud category.

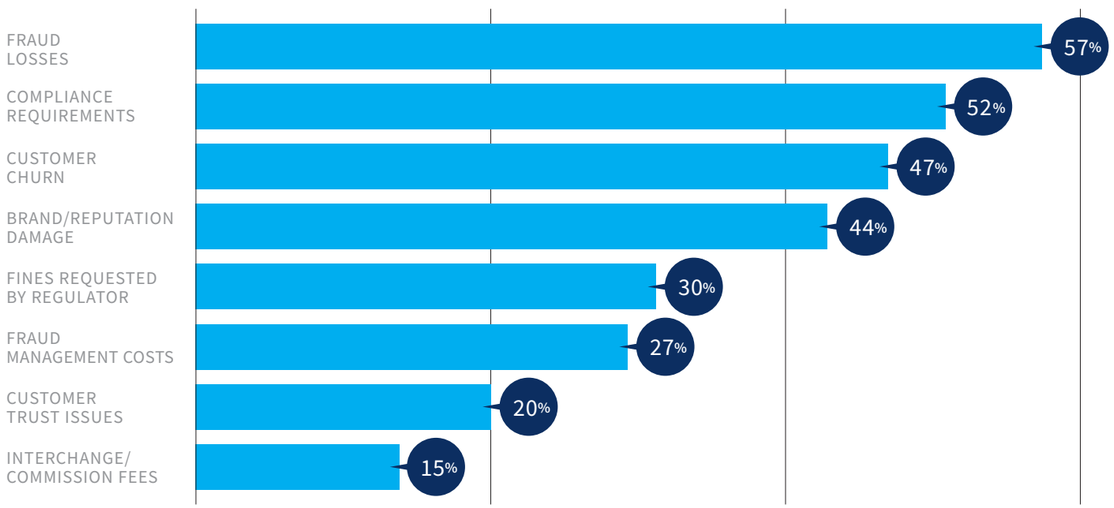


WHAT PERCENTAGE OF TOTAL FRAUD LOSS DO BONUS ABUSE, ACCOUNT RESELLING/SHARING AND SYNTHETIC/FAKE IDENTITIES REPRESENT TO YOUR COMPANY? (NUMBERS DO NOT ADD TO 100% DUE TO ROUNDING.)

What does gaming fraud cost North American operators?

Where fraud costs the most: direct losses, compliance and churn

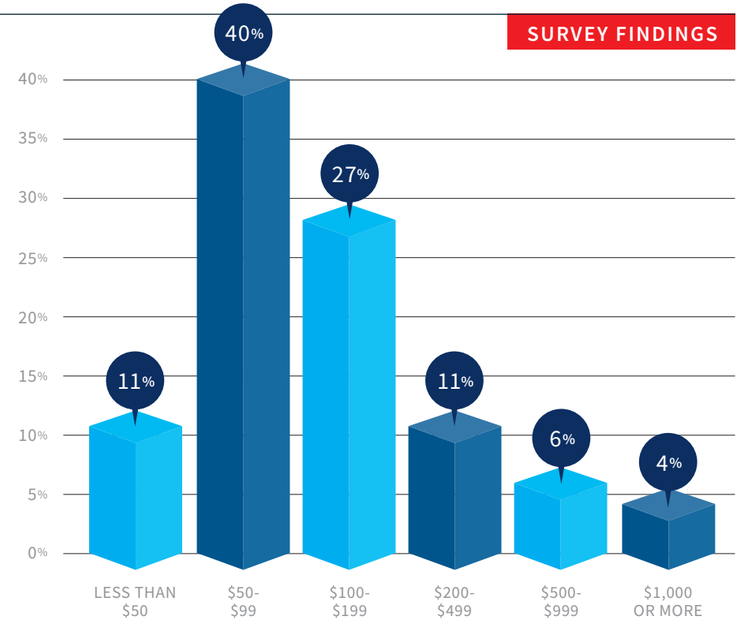
Respondents identified four business areas where fraud does the most damage: direct fraud losses (cited by 57%), increased compliance requirements (52%), customer churn (47%) and brand/reputation damage (44%).



TO WHAT EXTENT HAS FRAUD IMPACTED THE FOLLOWING AREAS OF YOUR BUSINESS? (RESPONDENTS COULD SELECT MULTIPLE RESPONSES.)

The cost per fraud: from less than $50 to over $1k

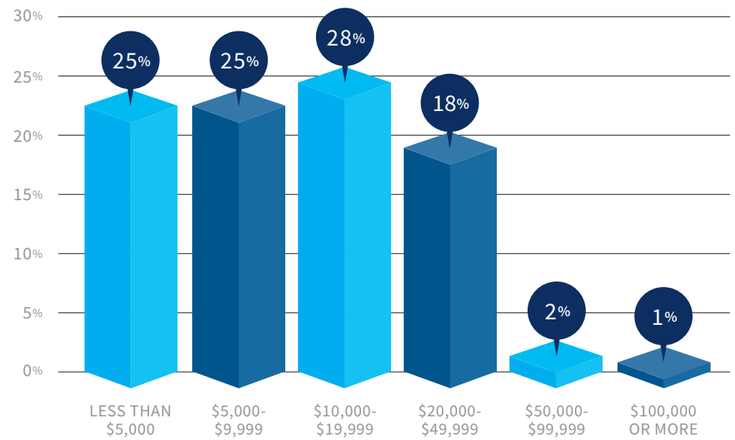
While two out of five respondents reported an average per-fraud cost of between $50 and $100, more than one in five reported their average per-fraud cost was $200 or more.



WHAT IS THE AVERAGE VALUE OF A FRAUDULENT TRANSACTION YOUR COMPANY DOES NOT PREVENT (IN USD)? (NUMBERS DO NOT ADD TO 100% DUE TO ROUNDING.)

The cumulative losses: $10k+ for about half of respondents

Looking solely at losses — not at the cumulative total of fraud exposure including prevented fraud — we discovered that more than a quarter of North American gaming operators are experiencing losses into the tens of thousands per annum.



WHAT IS THE APPROXIMATE VALUE OF YOUR COMPANY'S TOTAL FRAUD LOSSES (IN USD) DURING THE PAST 12 MONTHS? (AMONG RESPONDENTS WHO SUPPLIED A VALUE; NUMBERS DO NOT ADD TO 100% DUE TO ROUNDING.)

SPOTLIGHT ON BONUS ABUSE:

A damaging cycle of fraud

Why is bonus abuse the gaming fraudsters' sweet spot? Well, what makes taking advantage of customer incentives particularly appealing is the **rinse-and-repeat mechanics** of the fraud and the advanced tactics being made available to fraudsters. Here's a typical scheme in action:

So lucrative are these schemes that LexisNexis® Risk Solutions has detected bonus abuse networks responsible for fraud exposure as large as $3.2M. But how are fraudsters repeating this formula so successfully?

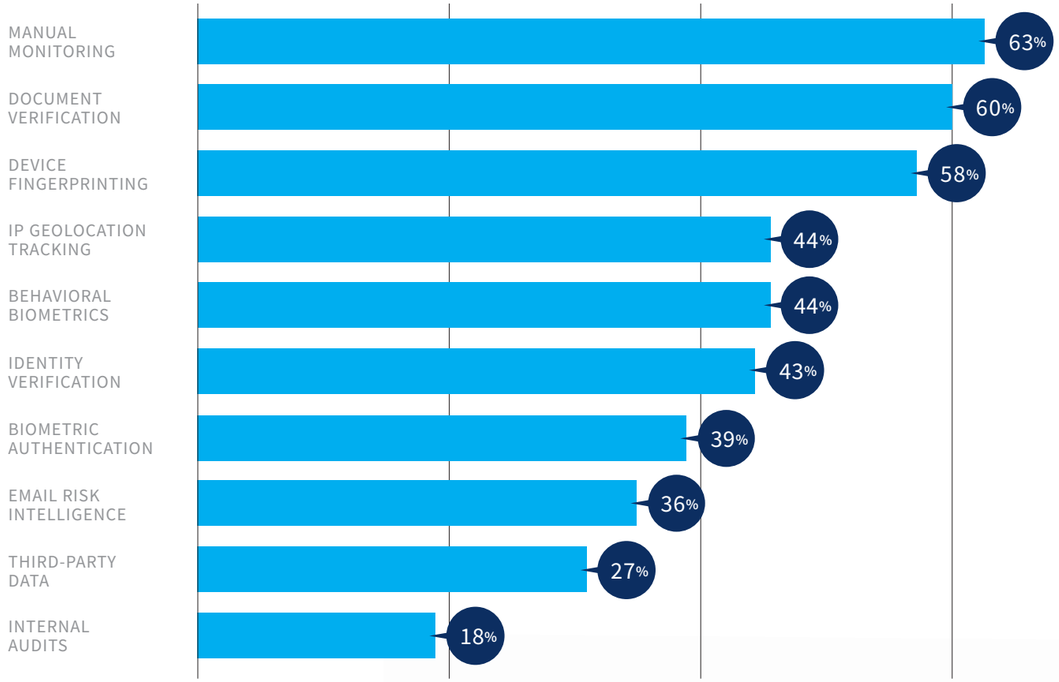
Kim Sutherland, Senior Vice President, Market Planning, explains:

'Gaming fraudsters conceal their locations and scale attacks by using VPNs and proxies to hide their true digital identity. Tracks are then covered using multiple devices never linked to the same email address, with criminal networks in place ready to exchange stolen gaming account details, match bets and continue the endless cycle of bonus abuse.

Leveraging global contributory networks and patented technology, we were able to link 95,000+ fraud events to just one instance of bonus abuse. This highlights the sophisticated collusion driving the fraud — and the collaboration required by the good guys to fight back.'

Read the ebook:
iGaming Bonus Abuse and How To Fight Back

Which anti-fraud measures are North American gaming operators backing?



WHAT TOOLS DO YOU USE TO HELP DETECT ACCOUNT RESALE OR SHARING. RESPONDENTS COULD SELECT MULTIPLE RESPONSES.

The fraud prevention choice: Multi-layered intelligence

Gaming companies overwhelmingly rely on six techniques to combat fraud: More than half employ manual monitoring, document verification and device fingerprinting; more than 40% utilize IP geolocation tracking, behavioral biometrics and identity verification.

The MVPs in user risk segmentation: Transaction history and behavior patterns

Nearly all respondents (94%) say they segment users based on risk profile as part of their anti-fraud tactics. But how does that risk segmentation take place? This pulse survey found transaction history and behavior patterns to be the most common, with device used not far behind.

26%	TRANSACTION HISTORY	12%	GEOLOCATION
26%	BEHAVIOR PATTERNS	8%	PAYMENT METHODS
22%	DEVICE USED	5%	REFERRAL SOURCE

WHICH FACTORS DO YOU CONSIDER WHEN SEGMENTING USERS? (MOST-CITED RESPONSES.)

How are they measuring success?

The two most important **fraud management KPIs** in our survey are loss reduction and customer experience improvement. Both top the list for about three out of every five respondents.

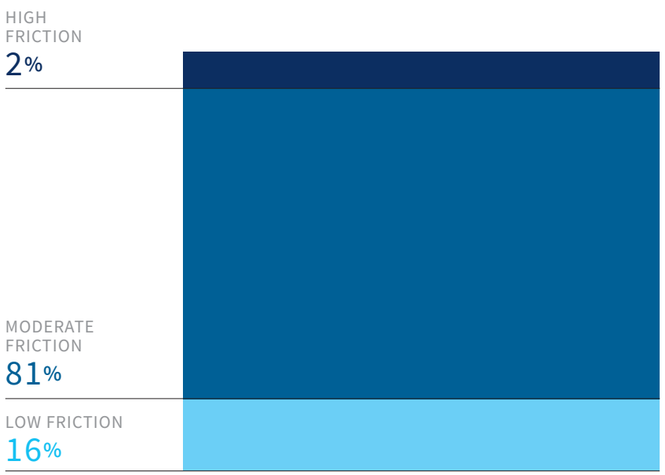
64%	FRAUD LOSS REDUCTION
56%	CUSTOMER UX IMPROVEMENT
46%	CHURN REDUCTION
35%	REGULATORY COMPLIANCE
35%	BETTER CONVERSION
29%	LOWER OPERATIONAL COSTS
14%	FASTER RESPONSE TIME

WHICH KPIS ARE MOST IMPORTANT WHEN MAKING DECISIONS ABOUT FRAUD MANAGEMENT? (SELECT UP TO 3.)

How does friction caused by fraud prevention impact customer experience?

How much friction scares away customers?

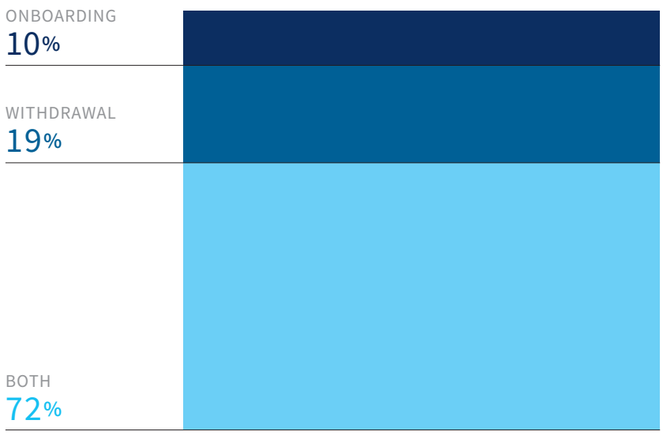
Aggressive anti-fraud strategies run the risk of alienating new customers and 81% of respondents say even moderate friction is enough to drive them off. Around two in three companies (65%) carefully monitor their friction level using customer surveys, a little higher than the global average (62%).



AT WHAT LEVEL OF FRICTION DO YOU OBSERVE USERS ABANDONING THE REGISTRATION PROCESS? (NUMBERS DO NOT ADD TO 100% DUE TO ROUNDING.)

When do abandonments happen?

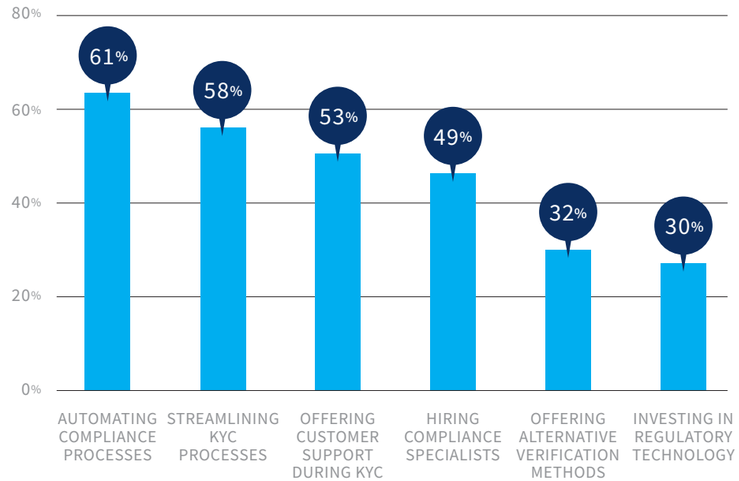
Gaming platform users can drop out at any point in the customer journey. Among our survey respondents, over two-thirds (72%) say platform abandonment happens both at onboarding and at withdrawal.



DO USERS TEND TO SWITCH TO COMPETITOR PLATFORMS IF THEY ENCOUNTER TOO MUCH FRICTION DURING [THESE PHASES]? (NUMBERS DO NOT ADD TO 100% DUE TO ROUNDING.)

KYC streamlining and process automation are keys to reducing regulatory friction

Compliance with regulations often leads to increased customer friction, an effect gaming companies are keen to manage. Automating compliance processes is their top technique, with streamlining KYC processes and offering customer support rounding out their top three.



HOW DOES YOUR ORGANIZATION MANAGE REGULATORY-RELATED FRICTION? (SELECT ALL THAT APPLY.)

Survey respondent insight:

"In the onboarding phase we have to be less restrictive, because first we need to understand the business that those players are bringing to understand if it's fraudulent or not."

CASE STUDY:

Stopping online gaming fraud at the door

A global gaming and gambling operator leveraged our unique blend of device, behavioral and email intelligence to prevent fraud without impacting genuine users, driving incredible results in the process.
Here's how they did it:

Fraudster
with stolen credentials

Attempts Account Creation

- Device showing a mismatch in typical behavior patterns
- Suspicious email domain detected
- Low digital trust score and short-lived identity data
- Lack of historical activity linked to provided account information

Account Creation Request is Flagged for Anomalies

- Discrepancies detected in account age, location and provided personal details
- Device has been linked to multiple accounts
- IP and geolocation mismatches raise red flags

Fraudster Attemps to Exploit the Newly Created Account

- Bulk promotional abuse, repeated sign-ups and testing stolen payment credentials flagged
- Transaction anomalies and unusual account activity detected

Fraudster Gets Stopped at the Door

- Risky accounts are flagged or blocked
- Trusted users, on the other hand, can continue playing without interruption

Their results:

86% **Reduction** in frauds misclassified as trusted

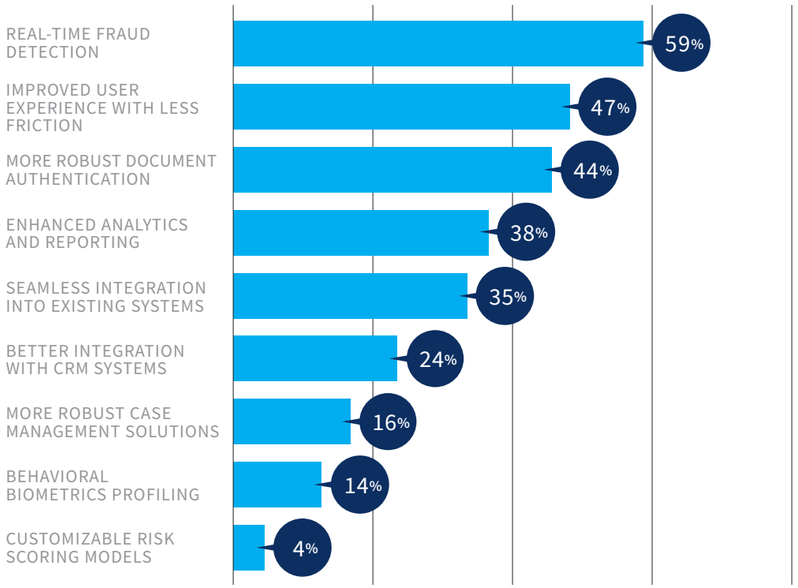
125% **Increase** in fraud detected at web sign-up

Did you know?
LexisNexis® Risk Solutions help businesses around the world streamline customer onboarding with advanced fraud detection, identity verification, document authentication and KYC solutions.

North American gaming fraud prevention: 2026 playbook

What fraud professionals want more of

Gaming companies want new tools to be able to detect fraud attempts in real time and they want a more frictionless experience for their customers. Other top features and capabilities they'd like to absorb include more robust document authentication, seamless integration and enhanced analytics, all of which were cited by at least a third of our respondents.



WHAT FEATURES OR CAPABILITIES WOULD YOU LIKE TO SEE IN FUTURE FRAUD MANAGEMENT TOOLS?

Where they need to improve

The inability to effectively detect multi-accounting ranks as the top concern in our weighted ranking, with a similar inability to detect stolen and synthetic IDs coming in a close second.

#1	MULTI-ACCOUNTING DETECTION
#2	STOLEN/SYNTHETIC ID DETECTION
#3	HIGH CUSTOMER CHURN
#4	BALANCING FRICTION & USER UX
#5	PRIVACY CONCERNS
#6	REGULATORY/COMPLIANCE CONCERNS
#7	SELECTING FRAUD SOLUTIONS
#8	TECH IMPLEMENTATION COMPLEXITY
#9	VALUE VS COST OF FRAUD PREVENTION
#10	DISTINGUISHING HUMANS VS BOTS

What they are going to prioritize

When listing their goals going forward, gaming companies prioritize inspiring customer loyalty by improving the user experience, with improving fraud management a close second.

#1	IMPROVE CUSTOMER UX & LOYALTY
#2	IMPROVE FRAUD MANAGEMENT
#3	BUILD TOPLINE GROWTH
#4	MINIMIZE BUSINESS & REGULATORY RISK
#5	REDUCE CHURN & ABANDONMENT
#6	IMPROVE BOTTOM-LINE PERFORMANCE
#7	IMPROVE WITHDRAWAL AUTOMATION
#8	ACCELERATE SHIFT TO DIGITAL BUSINESS
#9	MINIMIZE ONBOARDING FRICTION
#10	ACCELERATE RESPONSE TO CHANGES

Data in this section is global.

LEFT: HOW CHALLENGING HAVE THESE FRAUD PREVENTION CHALLENGES BEEN FOR YOUR TEAM OVER THE PAST 12 MONTHS? RIGHT: TO WHAT EXTENT IS YOUR ORGANIZATION PRIORITIZING THE FOLLOWING BUSINESS INITIATIVES DURING THE NEXT 12 MONTHS? (BOTH LISTS RANKED BY AGGREGATING MULTIPLE CHOICE ENTRIES.)

81%

Currently work with **four or fewer** fraud protection partners

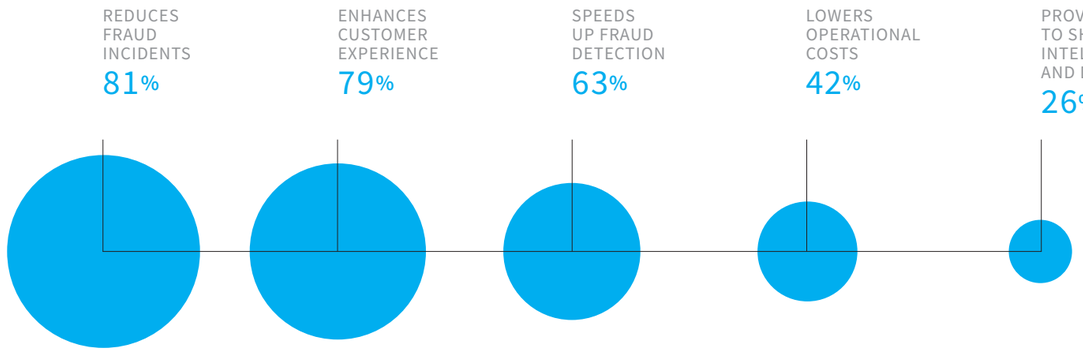
96%

Plan to **increase the number of partners** in the year ahead

Data collaboration: A fraud prevention slam-dunk missed in gaming?

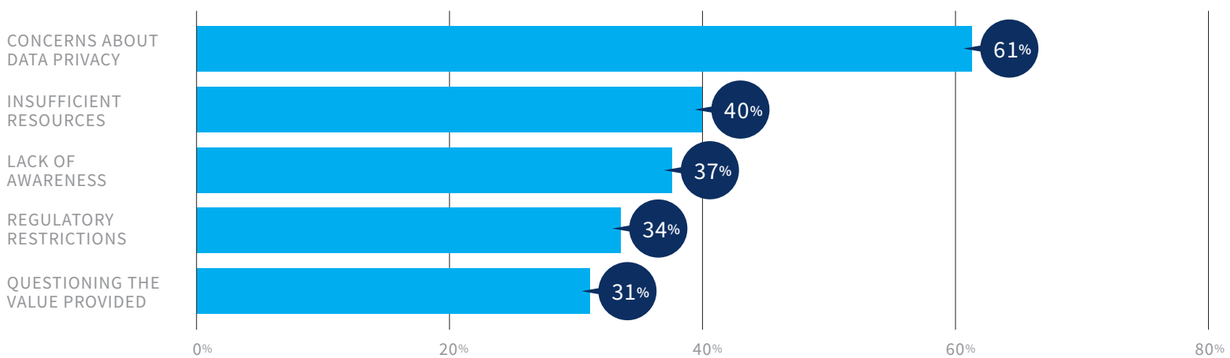
One in five are sharing data. Here's where they're seeing the benefit:

WHAT VALUE DOES THE NETWORK BRING TO YOUR FRAUD AND RISK MANAGEMENT?



Four in five aren't currently sharing data. Here's why:

WHAT ARE THE MAIN REASONS FOR NOT PARTICIPATING IN SUCH NETWORKS?



Responsible gaming is rising as an ethical and regulatory imperative:

"I found out from her profile and social media accounts that this one woman was 65 years old, living on a fixed income in a very modest home and she was spending beyond her means.

So I gave her a call. She's like, 'Oh, I'm just bored…I don't have anybody.' And it came out that she just really didn't have the money; she had a gaming problem. So I made a business decision that it just was not ethical to take money from this woman and closed her account. And she wrote a letter, she thanked us and she put herself in the self-exclusion list. Sometimes, you just have to pay attention and make that phone call."

– Gaming operator in North America

Conclusion

Online gaming fraud professionals in North America continue to strive to find the balance between security concerns and getting customers playing faster.

With fraud refusing to relent and adding friction simply not an option, they are seeking more advanced tools and partners capable of passively detecting fraud in real-time, preventing bonus abuse and streamlining regulatory requirements, such as automated KYC checks.

For these operators, frictionless user experiences and more robust document authentication join real-time fraud reduction at the top of their wish lists. It's part of a general acknowledgement that companies need to continuously up the ante when it comes to tackling multi-accounting fraud and stolen and synthetic identities.

Increase the thrill of the game. Shorten the odds on fraud.

Get trusted customers playing faster and keep your gaming and gambling ecosystem free from threats with advanced fraud detection analytics and powerful authentication and verification solutions.

FIND OUT MORE

LexisNexis®
RISK SOLUTIONS

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe. 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. For more information, please visit LexisNexis Risk Solutions and RELX. Our solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

This document is for informational purposes only and does not guarantee the functionality or features of any LexisNexis Risk Solutions products identified. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.