LexisNexis®
RISK SOLUTIONS

Health Care

E-BRIEF

Are your new enrollees who they say they are?

How to minimize member fraud during enrollment season.

2020

It’s almost enrollment season again

—and fraudsters are ready to add their own “members” to the mix

- Millions of people will join, switch and leave health plans. Some are following their doctors, some are choosing new employer-provided options and some are simply ready for a change.
- Every aspect of enrollment depends on identity data. Payers need to be able to verify that new enrollees are who they say they are—across all their various coverage options.
- There is alarming growth in criminals taking advantage of the enrollment process. An FCC report in 2019, showed more than 473 million health-related scam calls were recorded in October 2019—the start of open enrollment season.[1]

The average lifetime value of a “lost” health plan member can top **$100,000**[2]

Varying degrees of detail in patient data can make managing identities difficult.

10 million of the recently insured under health reform have no claims history[3]

5% of patients at any given facility have more than one active Master Patient Record[3]

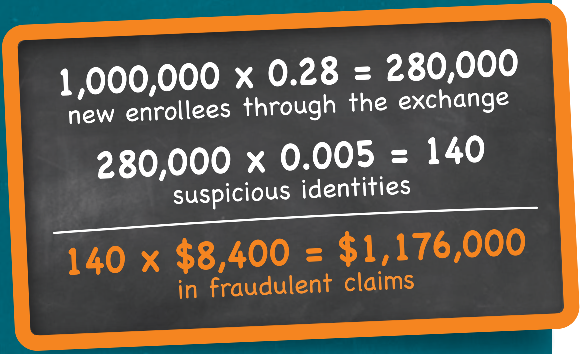
Payers need a data analytics partner with the tools—and the expertise—to stop fraudsters in their tracks

- Banning behavior that takes advantage of enrollment season has not eliminated fraudsters.
- Protecting against claims and other types of fraud—by keeping suspicious identities out of a payer’s enrollee mix—is now a relentless cat-and-mouse game of outwitting the perpetrators.
- Smart technology that helps spot potentially phony or inconsistent identity data at or before enrollment is your most powerful defense against enrollment season fraud.

Types and costs of identity fraud continue to mount

- Brokers enroll members without their knowledge for the commissions
- Plans overpay claims to fraudulent entities—and violations under the False Claims Act can result in fines up to three times the amount of the claim plus an additional $5,000 to $11,000 each
- Plans have to return premium payments

For example: Let's assume 28% of a plan's total enrollment of 1 million came through exchanges, and 0.5% of those enrollees submitted suspicious data. Their total claims—an average of $8,400, for example—could total almost $2 million. The fines the plan might pay could total more than $15 million when doubled. That's more than $17 million lost to one type of fraud.



1,000,000 x 0.28 = 280,000
new enrollees through the exchange

280,000 x 0.005 = 140
suspicious identities

140 x $8,400 = $1,176,000
in fraudulent claims

And even when outright fraud isn't the issue, data hygiene challenges can still be costly.

- Plans lose state Medicaid premiums because they can't reach members
- Payers are fined for being unable to provide enrollment materials in a timely manner

It's always important to verify member information, during enrollment season and every day of the year.

Criminals can't wait for enrollment season. Are you ready?

As activity ramps up during enrollment season, additional due diligence is required from payers.

- Unfamiliar players are demanding new kinds of access to and submitting different types of data on individuals. Payers' membership changes more than usual, and many enrollees have deadlines to meet.
- Fraudsters falsely add "members" to payers' enrollment systems—using a mix of real and fake information—in hopes those ineligible identities will get lost in the enrollment season shuffle and they can benefit from claims fraud or undeserved commissions.

Payers can't count on prohibition to safeguard the integrity of their member data and protect their enrollment systems from criminals creating identities out of an assortment of sometimes legitimate, sometimes stolen information. But they can fight back. Smart payers—teamed with a data analytics partner that specializes in identity data management—can beat fraudsters at their own game. When payers build in the right detection and alert processes, fraudsters start to stand out—enabling focused follow-up investigations.

The boom in enrollment season activity is built on identity data

Many of the individuals involved in open enrollment are new health plan members. Some of them have no previous coverage and no background data whatsoever, and some are switching from other plans or other payers. Many of the platforms new and returning enrollees use to submit identity information—plus the myriad providers, at multiple locales, of enrollment assistance—represent unfamiliar, and untested, new sources of data for payers.

A key challenge for payers: So much identity data submitted in such a short time

New players—and the new platforms they use to submit enrollment information—create fertile ground for fraudsters, leaving plans exposed to nefarious activity in both online and in-person transactions.

Payers have a way to approach the growing amount of fraud—and prevent it from happening

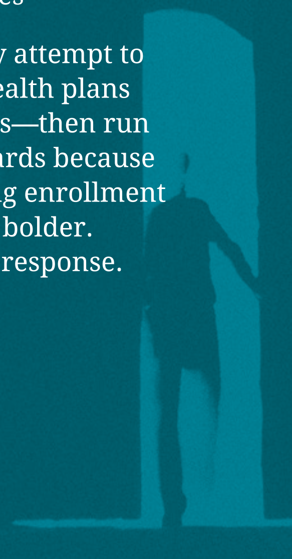
- A problem to watch out for is aggressive brokers trying to make up lost business. More and more people are cutting brokers out of the enrollment process because they can do it themselves. Some brokers that see a big hit in revenues may manipulate synthetic identity data—submitting enrollment information for minors or deceased or ineligible individuals to get commissions from payers.
- Another growing problem is enrollment fraud committed at rehabilitation centers, including some sobriety-based programs and even senior living facilities; fraudsters use actual patients' data to buy health insurance policies without their knowledge or permission, then submit false claims in their names—sometimes netting millions of dollars in a short time.
- Fraudsters also often assemble data piecemeal—using a date of birth from one source, for example, and falsifying the address to get undeserved benefits or better premium rates.

Reviewing mounds and mounds of identities during the enrollment season onboarding process to pick out those that are potentially high risk slows down onboarding, increases the manual resources required to review files, increases risk if any records aren't carefully reviewed for the sake of time and increases administrative verification costs.

Fraudsters infiltrate payers' enrollment data using stolen or synthetic identities

- Brokers collecting commissions by enrolling ineligible individuals
- Enrolling deceased individuals
- Enrolling fictitious individuals
- Enrolling minors
- Falsifying age and address to get unentitled benefits
- Receiving benefits under a fake or similar Social Security Number
- Providers submitting false claims in patients' names
- Providers self-enrolling patients
- Sharing member insurance cards to obtain controlled substances
- Lying about income to get Premium Tax Credits
- Setting up fake exchange websites
- Submitting enrollment information under multiple addresses

Aggressive fraudsters may attempt to enroll fake identities in health plans to get fake insurance cards—then run up treatment under the cards because they weren't caught during enrollment season. Criminals will get bolder. Payers must step up their response.



Efforts to stop identity theft haven’t entirely succeeded; in fact, identities have become a commodity. Identities are being stolen at an alarming rate:

The Equifax breach involved 143 million people.[4]

In 2019, 1,473 breaches exposed the personal identifying information of 164.7 million records.[5]

100 million records were exposed in the 2019 Capital One Financial Corp. breach.[5]

Patient medical records can sell for up to $1,000 depending on the information included.[6]

26% of all U.S. consumers have been impacted by healthcare data breaches.[7]

Swiping or making up an identity in another industry and using it in healthcare requires very little effort.

Additional scrutiny is critical. Health plans need to take action to protect themselves from criminals using stolen or synthetic data to create identities, make false claims and reap unearned rewards. The problem is getting worse every day.

Fight fire with fire: Technology solutions offer early fraud alerts

With so many data breaches being reported, the assumption is that the fraudsters have data. So it’s up to payers to keep them from using it.

- It’s imperative to protect against identity fraud by authenticating the identity of the individuals attempting to enroll or submit claims through brokers and exchanges.
- The costs in unwarranted claims, inappropriate commissions, fines and sanctions and premium returns could be enormous if the identity fraud is not caught in time.
- The process must both authenticate accurate individual identities and highlight contradictory or suspicious identity characteristics.
- And it must be able to efficiently evaluate each enrollment application quickly.

To fight fraud during enrollment season, payers need to quickly confirm that data being submitted by an individual is real and accurate—and that it belongs to the person seeking coverage. Once the information is confirmed, payers can compare it to the eligibility standards for their different plans.

That requires cross-referencing thousands and thousands of databases, current and historic, and piecing together and verifying multiple data points all at once—a seamless verification function at critical points in payers' workflow.

Payers can spot potential fraud without slowing the enrollment process

The results of that kind of verification include: significantly more insight into enrollees, beyond typical verification, and confirmation of both the validity and veracity of the individuals being enrolled—detecting potential identity fraud and speeding up the process of onboarding applications. InstantID® for Healthcare from LexisNexis® Risk Solutions is all about results, validating enrollment data being submitted, verifying individual elements of it and flagging compromised or suspicious identities. InstantID for Healthcare:

- Compares data elements against a vast store of data from public records, privately sourced data repositories and government lists
- Spots and fixes miskeyed elements—transposed numbers in an address, for example
- Provides indicators—maybe the ZIP Code belongs to a post office box—that detail the identity's potential risks

Then the solution provides a Comprehensive Verification Index score that indicates the level of identity verification assigned to each individual—helping payers focus their follow-up fraud investigation efforts.

Schemes to enroll ineligible identities are a 24/7 challenge for health plans, costing millions in losses every year from claims, commissions and fines, and enrollment season ups the ante.

Payers need to take advantage of the tools available to detect potential fraud this enrollment season and throughout the year.

For more information about LexisNexis Health Care, call 866.396.7703
or visit risk.lexisnexis.com/healthcare

LexisNexis® RISK SOLUTIONS | Health Care

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

Our healthcare solutions combine proprietary analytics, data science and technology with the industry's leading sources of provider, member, claims and public records information to deliver insights that improve cost savings, health outcomes, data quality and compliance.

[1] https://www.fcc.gov/health-insurance-scam-attempts-spike-during-open-enrollment

[2] Lexis Nexis Risk Solutions

[3] "ECRI Institute PSO Deep Dive: Patient Indentification Executive Summary, August 2016. https://www.ecri.org/Resources/Whitepapers_and_reports/PSO%20DDiveDeep%20Dive_PT_ID_2016_exec%20summary.pdf

[4] https://www.npr.org/2017/09/08/549549935/equifax-breach-exposes-personal-data-of-143-million-people

[5] https://www.iii.org/customprint/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[6] https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html

[7] https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time