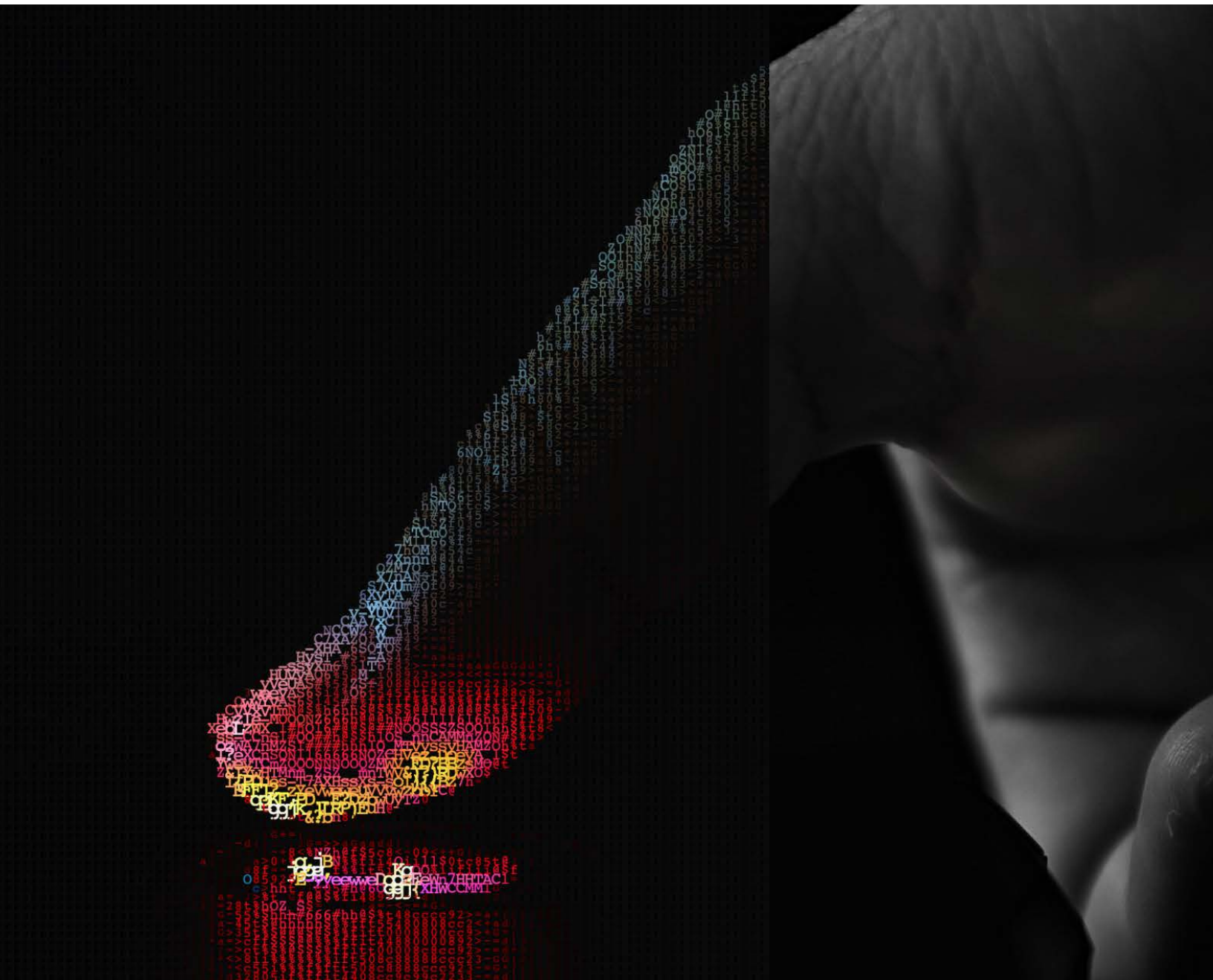
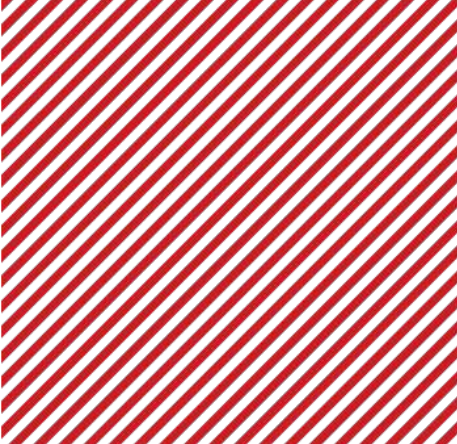


Reducing Insurance Fraud Through Enhanced Identity Verification



The insurance industry loses \$40 billion per year to fraud, according to the FBI.



“ Approximately 20 cents of every insurance premium dollar goes to covering the cost of fraud. ”

–North Carolina Insurance Commissioner, Mike Causey

Executive Summary

The insurance industry (excluding medical insurance) loses \$40 billion per year to fraud, according to the FBI.¹

Insurance fraud is one of the most common types of fraud. But the schemes perpetrated against insurance companies are vast, ranging from simple (issuing a fake claim) to more complex (enrolling and issuing claims on thousands of fictitious identities and/or unwitting victims). What is more, insurance companies face new challenges. Accelerated by the pandemic, firms increasingly rely on digital-first and digital-only environments to authenticate the identities of their customers and claims.

This white paper, developed by the identity and payments fraud experts at GIACT (a Refinitiv company), outlines sample insurance fraud schemes and how insurance companies can strengthen and streamline digital identity verification.

Insurance Fraud Landscape

It is estimated that fraudulent claims make up 10% of all underwriting losses among property and casualty (P&C) insurers.² Considering that U.S. P&C firms payout billions every year, the dollar figure that fraud extracts from these insurance fraud schemes is remarkably high.

According to consumer accounts, insurance fraud was responsible for nearly \$80B in losses in 2021.² Insurance fraud not only means higher operating costs and losses for insurance companies, but also higher premiums for consumers.

A part of the reason for insurance fraud's prevalence is the manifold ways in which insurance companies are exposed to fraud. For example, common insurance fraud schemes include inflating and “padding” claims, staging accidents or submitting false claims, to stealing identities or creating synthetic identities and submitting claims.

Most insurance companies are well aware that fraud is an issue. In fact, according to a survey, insurers admittedly believe at least 18% of claims contain some “element of fraud, inflation or misrepresentation.”³

10%

Fraudulent claims make up 10% of all underwriting losses among property and casualty (P&C) insurers

Insurers believe at least 18% of claims contain some "element of fraud, inflation or misrepresentation"

18%

What is clear is that validating that a customer is who they say they are represents both a challenge as well as an opportunity. Proper customer authentication can drive lower costs (in the form of less payouts for fraudulent claims) and better user experience (by creating a simultaneously safer and faster, more dynamic onboarding journey).

Are You Who You Say You Are?

Authenticating the true identity of a customer – i.e., asking: are you who you say you are? – has become more difficult than ever to get right. Following years of blockbuster data breaches, much of our personal identifiable information (PII) – from your name, SSN, DOB, phone and emails, etc. – is exposed on the Dark Web and is actively being used in identity-based attacks.

In fact, nearly half (47%) of all U.S. consumers have fallen victim to identity theft in the past two years, underscoring the issue of near-universal risk to every industry, including insurance.⁴ To commit identity fraud, fraud operators use a variety of methods, including:

- **True Name Fraud**

True name fraud is when a fraudster uses a victim's real data to commit fraud. Using legitimate PII, true name fraud can be difficult to detect. After successfully getting through the application process, the fraudster can execute a transaction, withdrawing funds into a controlled account, leaving the insurer holding the bag.

- **Synthetic Identity Fraud**

Synthetic identity fraud is when a fraudster combines real and fictitious PII to create an entirely new identity. Synthetic identity fraud attacks usually require patience; fraudsters will cultivate their synthetic identities over time, fostering them by creating accounts or opening credit cards or other accounts to establish a credit profile with a positive payment history. Once legitimacy and creditworthiness are established, the fraudster will 'breakout' and cash out on false claims.

- **Application Fraud**

Application fraud is the falsification of an application using fictitious or stolen identity data. This is done using true name fraud, synthetic identity fraud or some other form of identity theft. The goal of application fraud is to bypass the identity verification process at enrollment and continue on undetected.

- **Account Takeover**

Account takeover is defined as the unauthorized takeover of an existing, legitimate account. Directly following an account takeover attack, fraudsters can sit undetected for weeks or months, change the accounts banking information, cash out claims or make fictitious claims on behalf of a seemingly legitimate customer.

Surveying the Victims of Insurance Fraud

Insurance fraud has a long history. But over the past few years, fraud operations have learned to target different types of insurance policies using new and varied fraud tactics. According to a recent consumer survey, insurance fraud victims cite application fraud, account takeover and family and friendly fraud as tactics used against their insurance accounts.

Percent of Victims Whose Insurance Was Targeted by Applications Fraud



of victims say a health insurance plan was fraudulently applied for in their name



of victims say a life insurance policy or annuity was fraudulently applied for in their name



of victims say a P&C policy and/or claim was fraudulently applied for in their name

Percent of Victims Whose Insurance Was Targeted by Account Takeover



of victims say their insurance was used to file fictitious home, auto, or other insurance-related

Percent of Victims Whose Insurance Was Targeted by Family & Friendly Fraud



of victims say their insurance was used to file a medical or dental claim



of victims say their insurance was used to file a home, auto, or other insurance-related claim



of victims say their life insurance policy was cashed out

Source: Aite-Novarica, "U.S. Identity Theft: The Stark Reality," March 2021

Given the prevalence of fraud against insurance policies, many insurance firms are taking actions to mitigate theft. According to a recent survey, 71% of insurers said that they are looking to invest in technology to detect claims fraud.⁵

Included in this mix will be technology solutions that help insurers strengthen identity verification and the authentication of customer data.

Addressing Single-Point Solutions

One reason for the continued effectiveness of identity fraud is that organizations lack an equally effective approach to identity verification. Too often organizations apply a single-point, patchwork approach. That is, they emphasize safeguarding one aspect of the customer lifecycle — such as enrollment — while applying lesser controls (often in the name of customer experience) to another. But because fraudsters will migrate to whatever customer touchpoint is weakest, this type of single-point approach represents a significant vulnerability.

This patchwork approach often reflects the structure of an organization. Different departments have different functions and requirements. The unintentional result of this is the creation of siloes. For example, if one department isn't working closely enough with another, or using similar tools and programs that can communicate with one another, a fraudulent account can be passed on as legitimate. This example represents 'gaps' in the fraud prevention process which fraud operators purposely seek out and exploit.

To bridge these gaps, a holistics approach – i.e., one that manages the complete customer lifecycle, from enrollment to change event, to payment and ongoing due diligence – is needed.

Enhanced Identity Verification: A Holistic Approach

Insurance firms that want to enhance identity verification need access to better, more robust datasets that can be intelligently and easily applied throughout their organizations and the customer lifecycle. This includes:



Real-time access to a broader range of identity related data.

Insurers must have a system that accesses identity-related data with real-time updates. This data should be sourced from both traditional and non-traditional sources, such as email, social media, and digital marketing bureaus. When new information is added or updated, the data should reflect the change immediately. The real-time aspect is necessary to swiftly update when claimants have a new account, address, or update other items in the profile. A broader range of identity-related data ensures a safety net against fraudsters accessing and replicating information. In these ways, the tracking and maintenance of data is a proactive way to assess fraud risks before breakouts occur.



Advanced analytic and machine learning.

Analytics engines can help identify patterns in fraudulent activities. processes, a safer and faster customer experience can be achieved. Fraud operations can have common traits, and these can be sighted by analytics, given accurate and up-to-date data. This can be done before the payout of the claim, and sometimes even before a claim is filed or insurance policy is issued. Using analytics to recognize patterns in identity-related datasets allows for a swift process of discovering fraudulent applications and claims.



Broad integration and ease of access.

For data and analytics to make a difference, an integration that is easy to access and action upon need is needed. By integrating an enhanced, real-time identity verification solution into your existing processes, a safer and faster customer experience can be achieved. What is more, an identity verification integration that is brought to bear across the customer lifecycle –from underwriting to purchasing, and on an ongoing, automated basis – can significantly reduce the opportunity for fraud and reduce potential vulnerabilities. Integrations that allow for additional layers of authentication can also help mitigate identity risk –such as incorporating out-of-band authentication, further verifying identity through email or text.

About GIACT and the EPIC Platform

As the only financial technology provider that offers a complete set of enrollment, payment, identity, compliance and mobile solutions built on a single platform, GIACT's EPIC Platform is used by some of the largest insurance firms in the U.S.

Insurance firms use the EPIC Platform to enable faster onboarding and a better customer experience at enrollment while simultaneously managing fraud and risk; to proactively keep customer account data up-to-date and accurate to avoid identity-based fraud; to safeguard payments and reduce unauthorized returns through real-time; and to streamline compliance and reduce any opportunity for infractions, fines and enforcements.

The EPIC Platform's capabilities includes:

- Single API integration allows healthcare organizations to rapidly deploy customized solutions for enrollment, payment, identification, and compliance processes with minimal cost and operational disruption
- Positively identify patient accounts using multiple traditional and non-traditional data sources to improve underwriting, risk management, and KYC process
- Real-time account verification and authentication of patients and vendors, including funds verification, prior to enrollment or ACH payment processing to confirm status and verify funds availability before processing
- Minimize unauthorized ACH and check returns, which are costly and damaging to an organization's reputation
- Mobile authentication, identification, and verification in real-time across all patient touchpoints
- Real-time identity verification and authentication of scanned IDs and check payments



To learn how you can mitigate mortgage fraud risk with the **EPIC Platform**, speak to a GIACT representative today:
www.giact.com/demo

Citations

1. Thomson Reuters, "Identity Fraud's Impact on the Insurance Sector"
2. Coalition Against Insurance Fraud, "Fraud Stats," 2021.
3. Insurance Information Institute, "Insurance Fraud," Dec. 2015.
4. Aite-Novarica (underwritten by GIACT, a Refinitiv company), "U.S. Identity Theft: The Stark Reality," March 2021.
5. Coalition Against Insurance Fraud (underwritten by SAS), "2021 State of Insurance Fraud Technology Study"