What's next

Empresa

Mitigar el riesgo de fraude para obtener ayudas por desempleo con IA y biometría

En Europa y en Reino Unido los estafadores han aprovechado el caos generado por la COVID-19 para interceptar miles de millones de fondos de ayuda y estimulación económica. Ahora, los gobiernos y los bancos se preguntan: ¿Cómo podemos prevenir este fraude y proteger a los ciudadanos? Cada vez son más los que optan por soluciones inteligentes basadas en la IA y la biometría para detectar y prevenir de manera proactiva el fraude en el cobro de las ayudas al desempleo, sin dejar de garantizar que los solicitantes legítimos reciban sus prestaciones.

Simon Marchand
Posted 9 junio 2021

El negocio del fraude ya estaba en auge. Cuando la Comisión Europea hizo públicos los resultados de una encuesta realizada en la UE sobre “estafas y fraude” en enero de 2020, el informe reveló que la mayoría (56%) de los europeos había sufrido una situación de fraude en los dos últimos años.

Entonces llegó el COVID-19. El trastorno económico generalizado causado por la pandemia, creó nuevas oportunidades para los estafadores, sobre todo en términos de fraude en la obtención de ayudas al desempleo.

Con esta crisis, el mercado laboral de la UE se redujo drásticamente, con una pérdida récord de 5,5 millones de empleos en toda la zona durante el segundo trimestre del año. Pero a pesar de que los gobiernos se apresuraron a lanzar fondos de alivio y estimulación de la economía —desde los ERTE españoles, al programa “Furlough” de Reino Unido— el proceso de solicitud en algunos casos se optimizó para reducir la carga administrativa y que el dinero llegara a las manos de los ciudadanos afectados.

Los estafadores profesionales aprovecharon la situación rápidamente y presentaron reclamaciones de ayudas para empresas y particulares en nombre de otras personas y

compañías. En Francia estos criminales llegaron a hacerse con hasta 1,7 millones de € en pagos previstos para ayudar a las empresas con problemas derivados del COVID. En Alemania, las cifras ascienden a 31,5 millones de €, de un único gobierno provincial. Y en Reino Unido las estimaciones indican que hasta 3.500 millones de £ de ayudas para la COVID podrían haberse solicitado de manera fraudulenta o haber sido abonadas por error.

Todo ello no es más que una de las maneras en las que la pandemia del COVID-19 ha acelerado la necesidad de repensar cómo abordamos la autenticación y la prevención del fraude. Así, agencias gubernamentales de toda Europa están tomando nota de ello, dedicando más presupuesto a esos esfuerzos y están preguntando qué más pueden hacer para protegerse y proteger a los ciudadanos.

Una respuesta es la biometría basada en IA, que puede autenticar a los ciudadanos y atrapar rápidamente y de manera segura a los defraudadores durante las interaciones telefónicas y digitales. En comparación con las preguntas de seguridad o la validación teléfonica, la biometría es más rápida y más precisa a la hora de autentificar y detectar a los defraudadores porque se centra en el individuo, es decir, verifica a la persona basándose en quién es, en vez de hacerlo con algo que saben o que tienen. Incluso es mejor utilizar la biometría junto con otras funciones, como la detención del entorno (que verifica el dispositivo, la red, el canal y la ubicación) y medidas anti-spoofing (capaces de identificar números de telefóno y llamadas falsas, detectar voces sintéticas y reproducciones de audio).

Veamos un ejemplo: Un estafador llama a su call center decenas de veces, haciéndose pasar por diferentes personas cada vez para presentar solicitudes de prestaciones fraudulentas. Si el estafador dispone de los datos de la identidad de los ciudadanos (fáciles de encontrar en internet a través de las redes sociales y las Dark Web), puede pasar desapercibido y robar miles de euros en ayudas públicas.

Pero si dispone de una solución biométrica integrada en su contact center, reconocerá al estafador en cuestión de segundos y se generará una alerta para el operador en tiempo real. Mientras tanto, sus equipos de detección de fraude analizarán el historial de grabaciones de llamadas para identificar si la misma voz aparece varias veces en una serie de llamadas. De este modo, podrán añadir esa voz a la lista de alertas, de modo que el defraudador será detectado inmediatamente la próxima vez que llame, además de para recopilar pruebas de calidad que permitan construir un caso y denunciarlo.

Adaptarse a las nuevas realidades del fraude es fundamental a medida que recorremos los últimos coletazos de la pandemia y más allá. En plena transición hacia la “nueva normalidad” en 2021, los gobiernos deben dar pasos proactivos para proteger a los ciudadanos. Pequeñas inversiones en tecnologías de última generación, como la IA y la biometría, pueden ayudar a

optimizar y a proteger todas las interacciones de los ciudadanos, al tiempo que se les ayuda a acceder a las prestaciones más rápido y deteniendo a los estafadores en su camino.

¿Quiere saber más? Puede leer sobre las Soluciones de seguridad y biometría de Nuance o concertar una cita con un especialista para hablar de los desafíos en su organización y de cómo puede utilizar una tecnología como la biometría para solucionarlos.

Tags: biometría, fraude

More Information

Mejor prevención del fraude en las prestaciones por desempleo en todo el mundo.

Reúnase con el Responsable de prevención de fraudes de Nuance para una consulta personalizada de sus necesidades. Más información.

Engage us

About Simon Marchand

En la actualidad, Simon desempeña la función de Chief Fraud Prevention Officer para la división de seguridad y biometría en Nuance Communications. Simon es miembro Certificado de la Asociación de Examinadores de Fraude y posee una amplia experiencia en prevención de fraude, detección, seguridad y autenticación en los sectores banca y telecomunicaciones. Antes de Nuance, Marchand ocupó puestos de responsabilidad en los departamentos de prevención de fraude de compañías como Laurentian Bank y Bell, con sede en Montreal, y más recientemente en la Orden de Administradores Colegiados de Québec, donde dirigió su programa de inspección profesional. Marchand trabaja en estrecha colaboración con los clientes de Nuance para diseñar estrategias de autenticación y prevención de fraude basadas en tecnología biométrica que ayudan a detener a los criminales al tiempo que reducen el esfuerzo y la fricción de los clientes. Comparte regularmente su experiencia en diversas conferencias y asociaciones de todo el mundo y habla sobre los riesgos del fraude y el uso ético de la biometría en los medios.

View all posts by Simon Marchand