



El fraude digital aumenta en frecuencia y sofisticación

El aumento de los pagos digitales producido por un aumento de las ventas en canales online, ha provocado un aumento de los intentos de fraude, que un estudio de SAS cifra en casi un 35%.

Un informe de **SAS**, llevado a cabo **Javelin Strategy & Research**, desvela que los intentos de fraude han aumentado casi un 35% desde el inicio de la pandemia, lo que indica que los delincuentes son más activos en la invasión de los canales digitales. Los ciberdelincuentes también están aprovechando, según explica Manuel Rodríguez, especialista en fraude de la compañía en España, que las estrategias de control de fraude se basan en comportamientos de los consumidores que eran habituales y que se han visto modificados.

Según la firma, para combatir eficazmente el problema es necesario aprovechar un conjunto más amplio de datos digitales y un enfoque híbrido de múltiples capas para la toma de decisiones durante la pandemia y después de ella. La analítica avanzada es el común denominador que proporciona agilidad para el futuro.

Previsiblemente, los pagos digitales presentan un riesgo mundial cada vez mayor y, aunque las tecnologías de pago predominantes varían según la región, las tendencias del fraude tienen importantes similitudes geográficas. Esto indica que los delincuentes coordinan y comparten la información de manera más abierta que las instituciones financieras, lo que les da una ventaja significativa para prevenir los controles de fraude. El fraude transfronterizo es cada vez más común.

Además, el fraude digital está aumentando en frecuencia y sofisticación. Según el estudio, el arsenal de trucos de los estafadores y las redes delictivas se están volviendo tan avanzados como las tecnologías utilizadas para detectar sus actividades. La ingeniería social, el phishing, los esquemas de identidad, y una variedad de métodos de pago digital están cambiando las probabilidades a favor de los delincuentes. Las organizaciones deben ser conscientes de que los nuevos mecanismos de pago son una nueva diana para los hackers debido a controles ineficaces de mitigación de riesgos en el momento del lanzamiento.

Para la compañía, la complejidad de los vectores de ataque de los delincuentes requiere un enfoque por capas para prevenir y detectar el fraude, a la vez que se dispone de los medios para orquestar estrategias y actividades de investigación. Las acciones automatizadas y la gestión predictiva de casos basada en la inteligencia artificial y el machine learning pueden ayudar a reducir la dependencia del equipo para monitorizar las actividades de fraude y aumentar la eficiencia.

Por otro lado, aconseja que el uso de los datos para el análisis en tiempo real y las acciones automatizadas porque “será crucial para prosperar en esta nueva normalidad digital”. Los recursos varían en función de la madurez tecnológica, pero las organizaciones en todas las etapas tienen una necesidad común de obtener la mayor cantidad posible de datos en tiempo real para tomar decisiones eficaces. “La aplicación de la infraestructura de la nube para los sistemas de gestión del fraude aumenta los recursos para la ingestión de datos”, subraya.

Finalmente, recuerda que la transformación de los pagos, tanto en los métodos existentes como en los nuevos, requiere que las instituciones financieras comprendan todos los puntos de entrada de los pagos ya que su protección contra el fraude digital es considerablemente más complicada.

