백서

1조 달러 규모의 문제를 해결하기 위한 AI 기반 솔루션

글로벌 금융 산업의 신뢰 보호 및 사기 피해 방지

목차

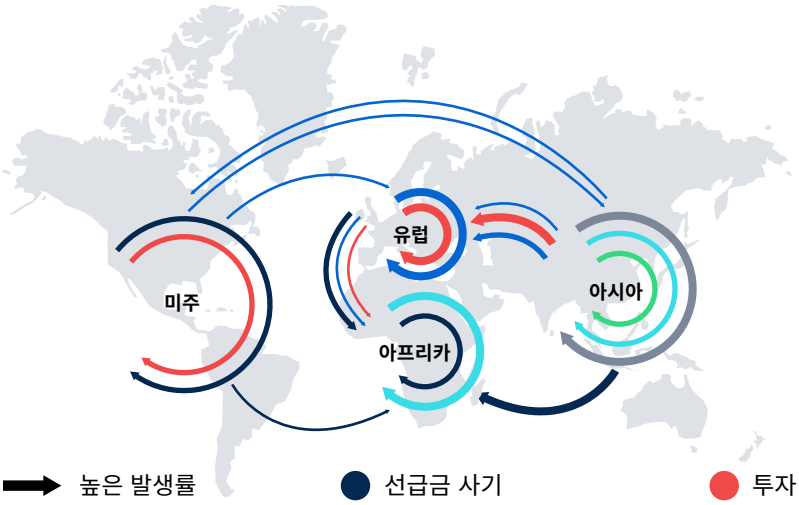
서문

사기 행위는 전세계 금융기관과 고객에게 점점 더 큰 위협이자 과제가 되고 있습니다. 금융산업은 막대한 금액이 오가기 때문에 여전히 사기의 주요 표적이 되고 있습니다.

최근 연구에 따르면 사기 표적이 되는 사람들의 비율이 세계적으로 증가하고 있으며, 사기와 부정 행위 시도 건수도 해마다 증가하고 있습니다. **글로벌사기방지연합(GASA)**에 따르면 2024년 전세계 사기 피해액은 1조 300억 달러를 넘어 사상 최대 규모의 재정적 손실을 기록했습니다. 또한 인터폴의 **2024 글로벌 금융 사기 평가 보고서(Global Financial Fraud Assessment 2024)**에 따르면, 국경 간 사기 피해액만 총 62억 달러에 달했으며, 그중 신원 도용, 피해자가 직접 승인한 송금(Authorized Push Payment, APP) 사기, 합성 사기의 비중이 가장 높게 나타났습니다.

글로벌사기방지연합 (The Global Anti-Scam Alliance, GASA)에 따르면 2024년 전세계 사기 피해액은 1조 300억 달러를 넘어 전례 없는 규모의 재정적 손실을 기록했습니다.

지역별 금융 사기 동향



출처: INTERPOL, Global Financial Fraud Assessment 2024

사기범들은 기존 수법과 신기술을 결합해 피해자를 더욱 정밀하게 노리고 있습니다. 탐지 능력 향상만으로 사기 건수가 감소할 가능성은 낮지만, 진보된 탐지 방식은 재정적 손실을 줄이는 데 도움이 될 수 있습니다.

사기 시도 수 자체를 유의미한 수준으로 줄이려면, 광범위한 대중의 인식과 강력한 보안 프로토콜이 필요하며, 이를 위해서는 사기 방지를 위한 다각적 접근이 필요합니다.

글로벌 위협 환경은 복잡하고 우려스러운 상황입니다. 그러나 상당한 우려 속에서도 긍정적인 변화가 진행 중입니다. 금융기관들은 사기 위협에 대응하고 은행, 고객 및 시스템을 방어하기 위해 머신러닝(ML)과 인공지능으로 구동되는 풍부한 데이터 소스와 실시간 의사결정 능력을 포함한 다양한 도구들을 늘려 나가고 있습니다.

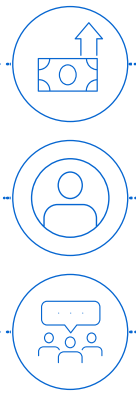
이 보고서는 글로벌 사기 동향을 검토하고, 금융기관이 직면한 문제들을 개괄하며, 은행 및 금융 기업들이 사기를 방지하고 조직과 고객을 보호하기 위해 활용하는 검증된 전략들을 제시합니다.

글로벌 사기 현황

법 집행 기관 또는 정부 기관에 신고한 피해자 비율 28%

$ 1.03조
글로벌 피해액

전세계에서 거의 절반이 주당 최소 한 번 이상 사기를 경험



4%
손실 회복 건수 비율

70%
미신고 피해자 비율

7%
불법 송금책이 될 수도 있다고 답한 비율

출처: Global Anti-Scam Alliance 2024 report

GASA 보고서에 따르면 소비자 인식 제고와 사기 예방·완화 노력 강화에도 불구하고 2024년 전세계 소비자의 거의 절반이 매주 사기 시도를 경험했습니다. 사기의 경제적·정서적 영향은 선진국과 개발도상국을 막론하고 거의 모든 연령층에 광범위하게 퍼져 있습니다.

사기 식별·저지의 신뢰도와 기술은 시간이 지남에 따라 향상되었지만, 사기 수법의 지속성과 정교함은 개인과 금융기관 모두에게 상당한 과제를 떠안기고 있습니다. 실제로 딜로이트 금융서비스센터는 미국에서 사기로 인한 손실이 연평균 32% 증가하며 2023년 123억 달러에서 2027년 400억 달러로 증가할 수 있다고 예측합니다.

전세계 피해자 중 **손실 회복 가능한 비율**이 고작 4%에 불과한 상황에서, 금융 사기의 피해를 완화하기 위한 예방 전략, 국제 협력 및 소비자 교육의 필요성은 그 어느 때보다 커진 상황입니다.

일반적인 고위험, 고손실 사기 유형

위험 범주	위험 설명	예시
비즈니스 이메일 침해 (Business Email Compromise, BEC)	사기성 송금으로 인한 재정적 손실	CEO의 이메일이 해킹되어 직원들에게 사기범의 계좌로 자금을 송금하라는 지시가 내려지는 경우
피싱 및 스피어 피싱	신원 도용, 재정적 손실 및 데이터 유출로 이어질 수 있음	직원이 회사 인사부서를 사칭한 이메일을 받아 자격 증명이 유출되는 경우
암호화폐 및 투자 사기	상당한 금전적 손실 및 사기	가짜 투자 플랫폼이 저위험 고수익을 약속한 후 투자자 자금을 가지고 사라짐
사칭 및 신원 도용	개인정보 오용 및 금융 사기	사기범이 피해자를 사칭하여 계좌를 개설하거나 대출을 받는 경우
조직을 대상으로 한 사회공학적 공격	데이터 유출 및 운영 중단	공격자가 IT 지원 담당자로 위장하고 직원에게 전화하여 자격 증명을 요구하는 경우.

출처: Federal Bureau of Investigation Internet Crime Complaint Center (IC3) Report, 2024

이 보고서는 주로 미국 데이터를 기반으로 하지만, 범죄가 미국과 연관성이 있는 경우(즉, 가해자, 피해자 또는 거래가 미국과 관련이 있는 경우) 전세계 누구나 미국 FBI의 인터넷범죄신고센터(IC3)에 신고할 수 있습니다. IC3는 2024년에 200개 이상의 국가로부터 신고를 접수했습니다.

사기 피해 방지를 위한 기술의 역할

사기 탐지 기술은 최근 몇 년간 크게 발전했지만, 대부분은 아직도 제1자 또는 제3자 사기와 관련된 기존의 위험 요소를 기반으로 합니다. 그러나 고객이 자신도 모르게 연루되는 사기가 증가하면서 사기 탐지도 이전보다 훨씬 더 어려워졌습니다.

위협 행위자들은 이제 신분 위조, 보이스 피싱 등의 사회공학, AI 기반 사기 등 새로운 수법을 사용하며, 경직되고 느린 기존 시스템으로는 효과적인 대응이 어렵습니다.

금융 거래의 속도와 복잡성이 증가함에 따라 이를 보호하는 도구 역시 발전해야 합니다. 이상 징후를 동적으로 탐지하고, 신종 위협에 적응하며, 현대 금융의 규모와 속도에 맞춰 운영할 수 있는 고급 AI 및 머신러닝 솔루션이 필요한 이유입니다.

세계적으로 펼쳐지는 사기와의 전쟁에서 첨단 기술이 강력한 무기로 부상하고 있습니다. AI, 머신러닝 및 데이터 기반 전략은 은행이 위협을 더 빠르게 탐지하고, 범죄 조직을 차단하며, 자산과 고객을 보호하는 데 도움을 주고 있습니다.

인간의 통제는 여전히 중요하지만, 다음과 같은 혁신 기술들은 세계적으로 더 안전하고 회복력 있는 금융 환경을 향한 강력한 길을 제시합니다.

> 데이터 기반 기술은 은행이 사기범을 저지하고, 범죄와 싸우며, 고객을 보호하고, 평판을 지키며, 수익을 보호하기 위해 신속하게 행동할 수 있도록 지원합니다.
>
> **→ 자세히 알아보기**

AI와 머신러닝을 통한 고급 탐지

전세계 금융기관들은 잠재적 사기를 암시하는 패턴, 이상 징후 및 행동을 분석하기 위해 AI와 머신러닝 기술을 점점 더 많이 도입하고 있습니다. 그러나 사기 범죄에 대항하는 데 이러한 도구의 효과를 극대화하려면 몇 가지 기본 요소가 먼저 마련되어야 합니다.

이 섹션에서는 사기 탐지 정확도를 높이는 동시에 오탐을 최소화하는 방법을 포함하여 이러한 첨단 기술을 효과적으로 배포하는 데 필요한 핵심 구성 요소를 살펴봅니다.

데이터 기반 체계

데이터 품질 및 다양성

금융기관은 모델을 효과적으로 훈련하기 위해 데이터의 품질과 다양성을 높은 수준으로 관리해야 합니다. 여기에는 다양한 사기 유형, 고객 접점, 사용자 행동 및 거래 패턴에 대한 명확한 라벨링과 보고를 제공하는 것이 포함됩니다.

모든 위험이 동일한 것은 아니며, 모든 사기를 똑같이 취급하면 만족스러운 결과를 얻을 수 없습니다. 탐지 과정에서는 현재의 채널별 경향을 넘어 디바이스, 고객 및 조직 정보와 같은 제3자 소스를 포함하는 다양한 실시간 데이터가 필요합니다.

피처 엔지니어링

은행은 사기 활동에 대한 인사이트를 제공할 수 있는 피처를(Feature) 데이터에서 식별하고 추출해야 합니다. 이러한 특성에는 거래 빈도, 위치, 디바이스 정보 및 사용자 행동 패턴이 포함됩니다.

탐지 및 모델링

이상 및 행동 탐지

기관은 데이터에서 비정상적인 패턴이나 이상치를 실시간으로 식별하기 위한 이상 탐지 알고리즘을 구현해야 합니다. 클러스터링이나 아이솔레이션 포레스트(isolation forest)와 같은 비지도 학습 기법은 정상적인 행동에서 벗어난 편차를 탐지하는 데 효과적입니다.

행동 분석

금융기관은 프로파일링을 통해 시간 경과에 따른 사용자 행동을 분석하는 모델을 개발해야 합니다. 이 접근 방식은 정상 행동에 대한 기준선을 설정하고 편차가 발생할 때 경보 또는 개입을 촉발합니다. 행동 분석은 특히, 피해자가 직접 승인한 송금(APP) 사기를 탐지하는 데 매우 중요하며, 키 타이핑 패턴이나 마우스 움직임과 같은 행동 생체 인식 기술은 디바이스 정보와 결합되어 사기 활동을 탐지하고 방지하는 데 도움이 됩니다.

머신러닝

지도 학습 알고리즘을 사용하여 라벨링/사기 태그가 지정된 데이터셋의 선택된 특성에 대해 모델을 훈련합니다. 이 모델들은 훈련 과정에서 학습한 패턴을 통해 거래를 정상 또는 사기 거래로 평가하는 데 활용할 수 있습니다. 의사결정 엔진은 더 정교한 사기 패턴을 정확히 식별하기 위해 위험 점수를 활용(및 실행)할 수 있어야 합니다.

고객 성공 사례

결제 사기 예측: 실시간 분석의 힘

"SAS를 통해 방대한 데이터를 처리하여 비정상적인 패턴을 식별하고, 사기 거래를 정상 거래에서 실시간으로 걸러낼 수 있습니다."

Jukka-Pekka Kokkonen, Nexi Group 사기 및 분쟁 담당 책임자

→ 고객 사례 확인

앙상블 기법

앙상블 기법(예: 랜덤 포레스트, 스태킹)을 통해 여러 모델을 결합하여 전반적인 정확도와 견고성을 향상시킵니다. 각 모델은 특정 유형의 사기 탐지에 특화됩니다.

운영 및 배포

실시간 처리

사기가 발생하는 즉시 탐지하고 방지하기 위해 실시간 처리 능력을 확보합니다. 적시 개입을 위해서는 실시간 의사결정 시스템에 분석 기능을 배포해야 합니다.

위협에 동시적으로 대응하는 능력은 결제의 실시간 특성을 보완하는 필수 요소입니다. 손실 방지를 위해서는 자금 이동과 관련된 현재 이벤트에 의사결정을 적용해야 합니다.

지속적인 학습

새로운 사기 수법에 대응하기 위해 지속적인 학습 메커니즘을 구현합니다. 새로운 데이터를 통해 모델을 정기적으로 업데이트하여 새로운 위협을 효과적으로 탐지합니다.

신뢰 및 보안

설명 가능성

사용된 머신러닝 모델이 해석 가능하고 설명 가능하도록 합니다. 이러한 투명성을 통해 사용자 간의 신뢰를 구축하고, 모델이 내린 의사결정의 근거를 이해할 수 있습니다.

다중 인증 (Multi-Factor Authentication, MFA)

다중 인증은 생체 인증, SMS 또는 이메일 확인과 같은 여러 계층의 검증을 추가하여 사기 탐지 능력을 강화함으로써 악의적인 행위자의 무단 접근을 방지합니다.

이러한 다중 계층 접근 방식은 적격한 사용자만 민감한 정보에 접근하거나 거래를 수행할 수 있도록 제한하여 사기 위험을 크게 줄여줍니다. 고객이 일반적으로 거래를 수행하는 주체이기 때문에 확인 메시지 이상의 조치가 필요합니다. 이는 고객이 거래를 진행하기 전에 먼저 생각할 수 있는 시간을 주기 위함입니다.

크로스 채널 분석

크로스 채널 모니터링은 온라인, 모바일 및 기타 플랫폼에 걸친 데이터 분석을 지원하여 잠재적 위협에 대한 포괄적인 시각을 제공하기 때문에 사기 탐지에 필수적입니다. 이러한 통합 접근 방식은 채널을 개별적으로 모니터링할 때 놓칠 수 있는 패턴과 사기 행위를 식별하는 데 도움이 됩니다.

클라우드 확장성

급증한 데이터 양과 새로운 위협에 신속하게 대응할 수 있게 해준다는 점에서 클라우드 확장성은 사기 모니터링에 필수적입니다. 이러한 유연성을 통해 사기를 적시에 식별하고 대응하여 잠재적 피해를 최소화할 수 있습니다.

베트남의 한 은행, SAS로 사기 탐지 시간을 단 몇 초로 단축

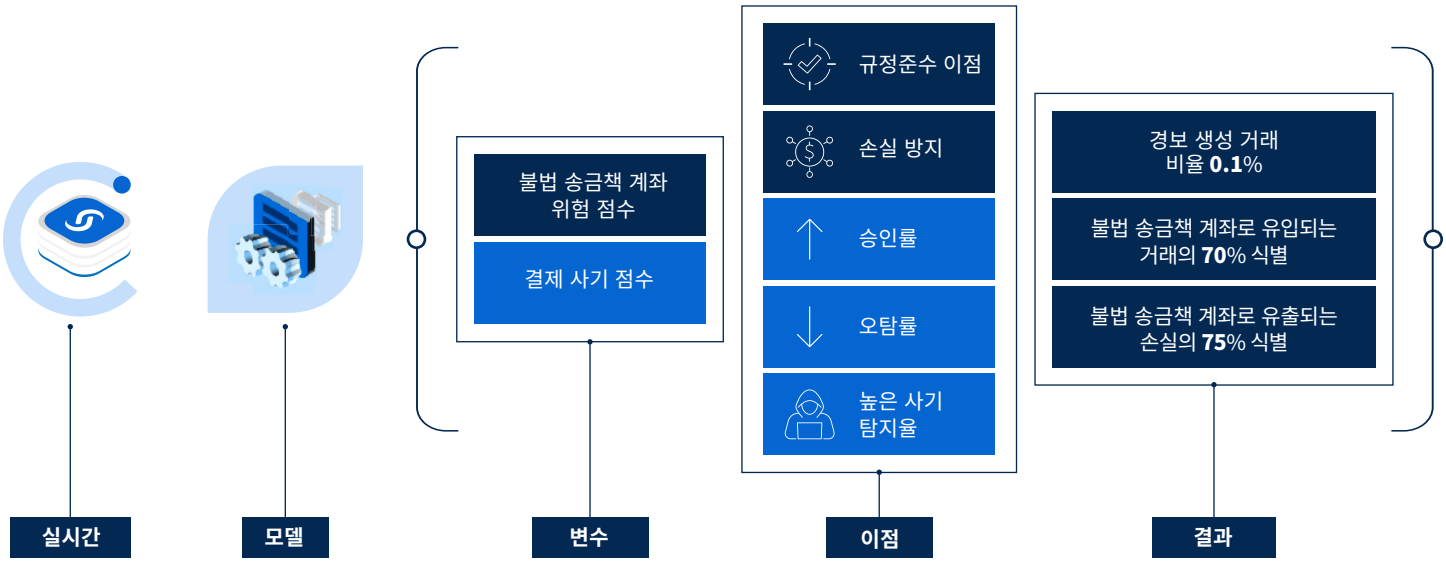
"실시간 의사결정을 위한 거래 스코어링 옵션을 사용하면 큰 효과를 볼 수 있습니다.오탐을 줄이고 분석을 지원함으로써 운영 효율성이 크게 향상되어 사기를 탐지하고 조사 시간이 크게 줄었습니다."

Joseph Vu,
Techcombank 기술 및 디지털 리스크 관리 이사

→ **고객 사례 확인**

고객 성공 사례

한 대형 금융기관은 SAS와 협력하여 사기 탐지 기능을 실시간으로 유지하면서 불법 송금책 계좌로 이동되는 자금을 식별했습니다. 이 다이어그램은 해당 프레임워크의 구조를 보여줍니다.



효과적인 사례 관리 및 고객 지원

효율적인 사례 관리는 신속한 탐지, 대응 및 피해자 지원에 필수적입니다. 사례 관리 도구는 조직에 위험을 초래할 수 있는 사건 정보를 추적하고 팀 간 협업 및 보고서 생성을 지원하는 체계적인 환경을 제공합니다. 주요 이점은 다음과 같습니다.

- 사기 확대를 방지하는 조기 탐지.
- 위험 심각도에 따른 최적화된 자원 배분.
- 의심스러운 활동을 차단하거나 중단하기 위한 신속한 대응.
- 효과적인 지원을 제공하는 투명한 처리를 통한 고객 신뢰 강화.
- 보고 요건에 따른 규정준수.
- 사건 분석 및 피드백을 통한 지속적인 개선.
- 내부 협업 및 외부 파트너와의 협업 촉진.

고객 성공 사례

CNG Holdings는 SAS를 통해 사기를 탐지하고 방지하면서 최적의 고객 경험을 제공합니다.

"신규 고객의 경우 90%가 훨씬 넘는 매우 높은 비율의 고객에 대해 신용 신청 절차를 거칩니다. 따라서 오탐이 거의 발생하지 않습니다."

Rick Cooney, CNG Holdings 사기 및 신원 관리 부사장

→ 고객 사례 확인

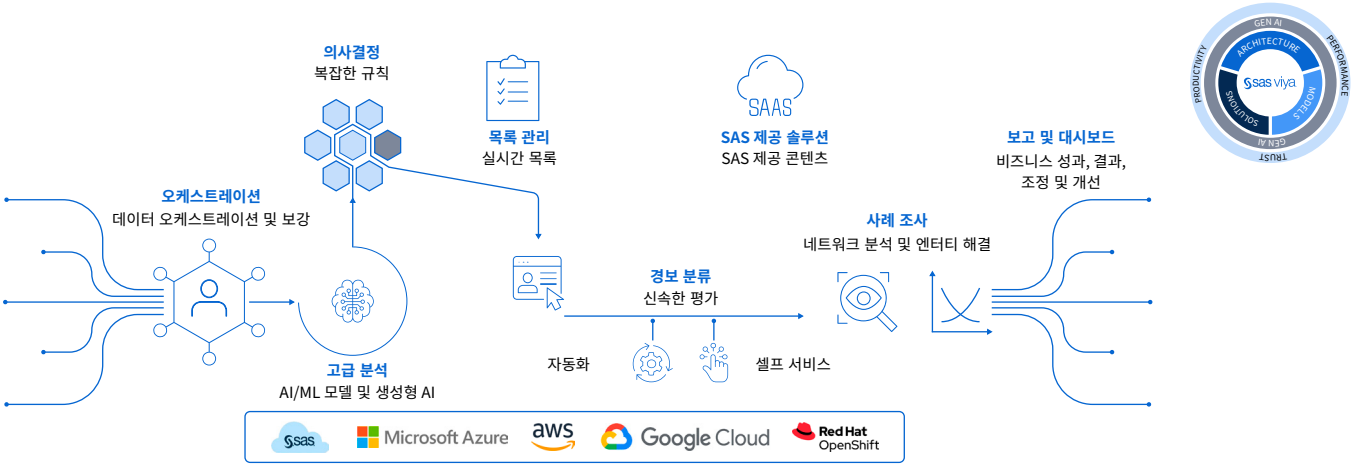
기타 모범 사례 및 협력 노력

사기 위협을 방지하기 위해 전세계 조직은 기술 발전과 혁신적인 솔루션 외에도 다음과 같은 요건을 충족해야 합니다.

- 국경을 초월한 위협 정보 공유로 국경 간 사기를 식별하고 차단합니다.
- 국제 규정 및 표준에 대한 최신 규정 준수를 유지합니다.
- 일반적인 사기 및 예방 조치에 대한 인식을 높이기 위해 고객 교육 캠페인에 투자합니다.

SAS의 지원 방식

엔터프라이즈 사기 관리 구성 요소



당사의 강력한 클라우드 네이티브 사기 의사결정 솔루션은 AI 및 머신러닝을 사용하여 실시간으로 사기 공격을 탐지하고 방지합니다. 이 플랫폼은 경보 관리, 사례 조사, 자동화 및 예측 분석을 포함한 여러 기능을 통합하여 금융기관이 새로운 위협에 신속하게 대응하고 위험 노출을 줄일 수 있도록 지원합니다.

SAS 사기 및 규정준수 솔루션은 은행 및 금융기관이 다양한 사기 유형을 식별하는 동시에 협업, 규정준수 및 지속적인 고객 교육을 촉진하여 사기 활동에 대한 탄력적인 방어 체계를 구축할 수 있도록 지원합니다.

이 모든 것의 중심에는 전세계 금융기관에 힘을 실어주는 클라우드 네이티브의 고성능 엔터프라이즈 사기 관리 솔루션인 **SAS Fraud Decisioning** 이 있습니다. SAS Fraud Decisioning은 내외부 소스 데이터를 최대한 활용하고 AI 및 ML 모델을 적용함으로써 사기로 인한 위험을 식별하고 즉각적인 대응을 가능하게 합니다. 주요 기능:

- 교차 위험 기반 조사 도구
- 비즈니스 인텔리전스 대시보드
- 크로스 채널 및 국경 간 위협 분석
- 데이터 오케스트레이션 및 보강
- 실시간, AI 기반 대규모 의사결정
- 신속한 경보 관리
- 노코드/로우코드 사용자 인터페이스

이러한 기능들을 통합함으로써 조직은 "큰 그림"을 파악하고 사기 위험을 사전에 탐지하며 대응 속도를 높일 수 있으며, 이는 새로운 위협을 해결하는 데 매우 중요합니다.

고객 성공 사례

태국의 한 은행, 실시간 사기 탐지 관리로 고객 보호

"SAS를 사용하면서 사례 경보량이 40% 줄고, 사기 탐지율이 35% 향상되었으며, 오탐이 18% 감소했습니다. 오탐이 줄고 SAS의 예측 스코어링 모델을 사용하면서 더 많은 사기를 탐지하여 향상된 고객 경험을 제공할 수 있습니다."

Pramote Lalitkitti, Krungsri Consumer 사기 관리 부문 수석 부사장

→ **고객 사례 확인**

SAS를 통한 사기 공격 방어

사기 범죄는 유형과 복잡성이 매우 다양하기 때문에 하나의 접근 방식으로는 모든 과제를 해결하지 못합니다.

이 과제를 성공적으로 해결하려면 고객을 적절하게 온보딩하고 고객 확인 프로그램을 유지하는 것부터 거래를 모니터링하고 특정 대상에 맞춤화된 교육 및 인식 캠페인을 시행하는 것에 이르기까지 다양한 기법과 접근 방식을 채택해야 합니다.

SAS는 사기 공격에 대응하기 위한 종합적인 접근 방식을 제공합니다. **SAS® Viya®**기반의 **SAS Fraud Decisioning**은 클라우드 네이티브 클라우드 애그노스틱 플랫폼에서 실시간 데이터 보강, 오케스트레이션 및 의사결정, 모델 관리, 거버넌스 및 개발, 신속한 경보 분류, 사례 관리, 대시보드 및 보고 기능을 모두 제공합니다.

금융 범죄 탐지 및 방지를 위해 SAS를 선택해야 하는 이유

SAS는 수십 년간 비즈니스 문제에 고급 분석을 적용해 온 경험을 바탕으로 사기 및 금융 범죄를 탐지하고 방지하는 검증된 플랫폼을 제공합니다. 전세계 수많은 금융기관들은 SAS를 통해 채널 전반에 걸친 위험 모니터링, 실시간 위협 탐지, 규제 요건 준수를 수행합니다. 머신러닝과 AI를 심층적인 도메인 전문성과 결합함으로써 SAS는 금융기관들이 새로운 사기 유형에 선제적으로 대응하고 고객 신뢰를 유지할 수 있도록 지원합니다.

SAS를 선택한다는 것은 글로벌 금융산업 전반에 걸쳐 혁신, 확장성 및 성과로 명성을 얻은 신뢰할 수 있는 파트너를 얻는 것입니다. SAS는 다음과 같은 광범위한 사기 문제에 대응할 수 있는 역량을 제공합니다.

- **결제 사기:** 업계 최고 수준의 데이터 분석 및 머신러닝을 활용하여 결제, 비금전적 거래 및 이벤트를 모니터링함으로써 결제 사기 위협을 실시간으로 정확하게 탐지할 수 있습니다.
- **계정 탈취 사기:** 고객 활동과 계정 관리 이벤트를 채널 전반에서 신속하게 모니터링하여 금융기관이 규제 위험에 노출되기 전에 불법 송금책 및 퍼널 계정을 탐지합니다.
- **신원 확인 및 인증:** 기존 신원 확인 방식을 넘어 신규 고객 관계에서 합성 사기를 더 빠르게 포착하고 신원 정보 일부가 위조된 것으로 의심될 경우 즉각 조치합니다.
- **신청 사기:** 수동 심사 비율을 낮추고 자동 승인 처리는 확대하면서, 신규 여신 신청에 대한 리스크를 정밀 평가하여 집금 계좌 및 고의 부도 사기를 사전에 차단합니다.
- **전자상거래 사기:** 판매자와 제3자 결제 처리업체 전반에 걸친 사기성 거래를 탐지합니다.

SAS의 차별점은 **채널 간 사기 탐지를 통합**하고, **설명 가능한 AI**를 활용해 규정 준수를 지원하며, 신종 위협에 신속히 대응하는 능력입니다.

세계 최대 금융기관들에서 **검증된 성과**를 바탕으로 SAS는 은행이 금융 범죄자들보다 한 발 앞서 나가는 데 필요한 기술과 전문성을 제공합니다.

고객 성공 사례

The Bank of East Asia, SAS를 통해 결제 사기 탐지 및 방지

"모든 거래에 대해 실시간 스코어링 및 의사결정을 수행하여 잠재적 결제 사기 활동을 조기에 탐지하고 예방할 수 있습니다."

Agatha Woo, The Bank of East Asia 담보대출 및 혁신 부문 책임자

→ 고객 사례 확인

SAS가 데이터, 탐지 및 의사결정을 연결하는 방식

1. 거래 모니터링 및 분석:
100%의 거래 및 고객 상호작용을 실시간으로 모니터링할 수 있는 능력은 복잡한 분석과 고급 탐지를 가능하게 하여 포괄적인 위험 커버리지와 규정 준수를 실현합니다.

2. 네트워크 링크 분석:
네트워크 기반 특성 및 시각화를 생성함으로써 숨겨진 관계를 신속하게 발견하여 범죄 네트워크의 구조를 파악할 수 있습니다.

3. AI 및 ML 역량:
당사의 데이터 사이언스 플랫폼을 통해 AI 및 ML 모델을 구축, 배포, 관리 및 확장할 수 있습니다. 그래프 분석, 행동 모델링, 비지도 이상 탐지를 단일 시스템에서 결합하고 원활하게 운영 환경에 배포하여 탁월한 탐지 정확도와 모델 갱신 속도를 달성합니다.

4. 지속적 모니터링:
엔터티별 맞춤형 위험 식별 전략은 네트워크 특성, 이상 탐지 및 행동 편차를 ML 모델에 입력하여 정확한 위험 식별과 개인화된 대응을 가능하게 합니다.

8. 엔터프라이즈 오케스트레이션:
SAS는 스트림, 실시간 또는 배치 방식의 데이터 피드 전반에 걸쳐 엔터프라이즈 위험 커버리지를 오케스트레이션합니다.
소스 및 제3자 데이터 또는 위험 엔진으로부터 데이터 품질을 통합 및 관리하여 고객, 거래 및 비거래 데이터를 보강합니다.
더 정확한 정보 기반 위험 의사결정 모델을 실행하여 커버리지를 높이고 오탐을 줄이는 고품질 경보를 생성합니다.
사례 관리 및 자동화 기능을 통해 경보 발생부터 해결까지 위험을 관리합니다.

7. 설명 가능성 및 해석 가능성:
적용된 모델 해석 가능성, 감사 추적, 고급 데이터 시각화 기능 및 조정된 워크플로를 통해 모든 이해관계자에게 의사결정 과정을 설명할 수 있도록 보장함으로써 의사결정에 대한 신뢰도와 위험 전략의 효과를 높입니다.

6. 자동화된 고객 확인:
전통적 속성, 링크 및 행동 기반 고객 위험 등급을 지속적으로 모니터링 및 업데이트하여 CDD팀의 조기 식별 및 주의를 유도합니다. 고객 유치부터 고객 생애주기 전반에 걸쳐 이 프로세스를 자동화하여 위험을 줄이고 운영을 간소화합니다.

5. 교육: 프로파일링을 통한 인식 및 역량 강화 최적화 과정을 간소화하여 조직이 맞춤형 교육 접근 방식을 구현할 수 있도록 지원합니다.

SAS 소개

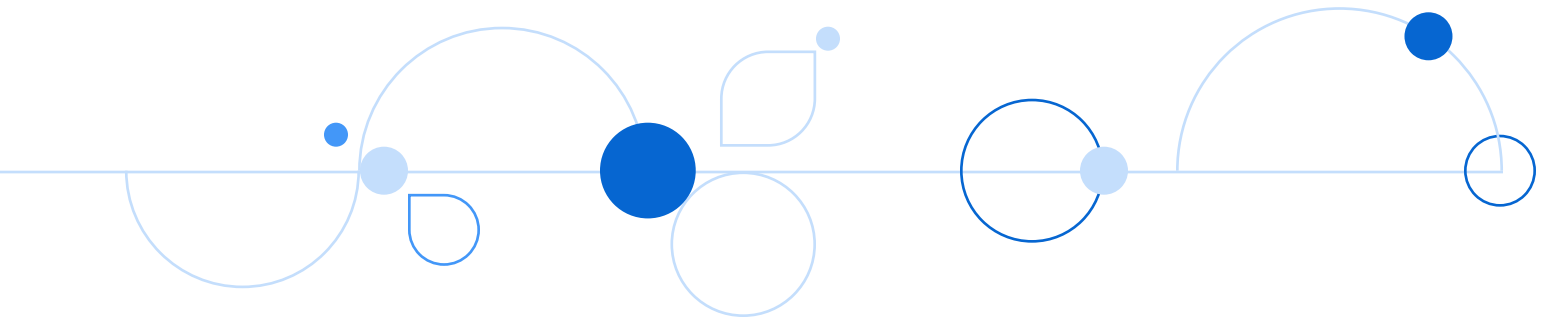
SAS는 데이터 및 AI 분야의 글로벌 리더입니다. 당사의 글로벌 전문가팀은 수십 년간 축적된 업계 경험을 바탕으로 전세계 92개국 1,600개 이상의 은행 및 금융기관과 협력하고 있습니다. 실제로 글로벌 100대 은행 중 90개 이상이 SAS의 고객입니다.

SAS는 비즈니스의 모든 측면에서 의사결정을 가속화하는 **뱅킹 분석 솔루션**을 제공합니다. 당사의 실시간 분석 및 고급 AI와 머신러닝은 금융기관이 위협을 조기에 탐지하고, 신종 위험에 대응하며, 고객 충성도를 높여주는 원활한 고객 서비스를 제공하는 데 도움을 줍니다.

다음 단계

SAS Fraud Decisioning에 대해 알아보세요.

독립적인 외부 분석가들이 SAS를 **엔터프라이즈 사기 / 결제 사기 솔루션 및 사기 방지 플랫폼 등 다양한 분야**에서 지속적으로 선도 기업으로 선정하는 이유를 직접 확인해 보세요.



자세한 내용은 sas.com/fraud에서 확인하세요.