소비자를 대상으로 하는 디지털 채널의 위험 관리

RSA FRAUD & RISK INTELLIGENCE SUITE

개요

개인이 그 어느 때보다 더 많은 방식으로 상호 작용하고 거래하면서 소비자 세계는 역사적인 변곡점을 맞았습니다. 조직은 소비자의 편의에 대한 요구를 충족시키기 위해 점점 더 많은 디지털 채널을 소비자에게 노출시켜 디지털 혁신을 추진하고 있습니다. 결과적으로 조직은 법률적 부담에서 신규 진출 업체와의 경쟁, 부정 행위자 및 사이버 범죄자에 의해 악용될 수 있는 잠재적 취약성 증가 등 전례 없는 비즈니스 및 보안 위험에 직면하게 됩니다.

이러한 소비자 분야의 변화는 의료부터 보험, 판매업체, 그리고 다음과 같은 대규모 중단을 직면한 금융 기관에 이르기까지 다양한 유형의 조직에 영향을 미칩니다.

- **편의성과 속도에 대한 고객의 기대치 증가**—고객은 디바이스 종류, 시간에 관계없이 정보에 액세스하기를 원하며, 신속하고 원활하며 개인화되고 채널에 구애 받지 않는 안전한 방식으로 디지털 거래가 실행되길 바랍니다.
- **핀테크 혁신**은 디지털 서비스를 제공하는 새로운 경쟁으로 이어지고 있습니다. 따라서 조직은 전략을 재고하고 API 경제 기반의 새로운 파트너십을 창출해야 할 뿐만 아니라 관리해야 하는 타사의 위험도 도입해야 합니다.
- PSD2, GDPR, SEPA 및 FFIEC와 같은 **광범위한 글로벌 규정**으로 인해 소비자 데이터 보호, 보안 및 프라이버시에 대한 책임이 높아지고 있습니다.
- 3DS 지원 환경인 "Faster Payments"(전 세계적으로 다양한 모양과 형태로 제공)를 통해 판매업체 트래픽을 유발할 것으로 예상되는 EMV 3D-Secure과 같은 **결제 혁신**, 대중 결제 애플리케이션 및 기타 핀테크 애플리케이션이 디지털 결

RSA FRAUD & RISK INTELLIGENCE SUITE

- 불편함 없이 **믿고 이용할 수 있는 제품**
- 고객이나 매출이 아닌 **부정 행위 감소**
- 모든 디지털 상호작용의 **위험 노출**
- 집단 인텔리전스를 통한 **분석 정보 최적화**
- 부정 행위 작업의 **효율성 향상**
- **사이버 범죄를 앞서가는 제품**

제량의 급격한 증가를 촉진하고 있습니다. 따라서 디지털 채널을 통해 송금되는 총 금액의 가치가 증가하여 조직은 더 많은 잠재적인 부정 행위로 인한 손실에 노출되고 있습니다.

- IoT(Internet of Things)를 통해 *Alexa*와 같은 다양한 디바이스가 소비자를 대신해 여러 활동을 수행할 수 있어 사실상 결과적으로는 계정 소지자의 ID가 사라졌으나, 그럼에도 조직은 정상 디지털 상호작용과 부정 디지털 상호작용을 구분할 수 있어야 합니다.
- 조직이 **전방위적 전략**을 수행함에 따라 잠재적인 침해와 취약성이 계속 증가되고 있습니다. 새로운 각 채널은 재무에 대해 더 효율적이고 간소화된 액세스를 제공하지만 이와 동시에 잠재적 보안 취약성도 창출합니다.
- **디지털 활동과 거래 볼륨의 급격한 증가**는 부정 행위를 완화하고 조사하기 위한 조직의 최소한의 성장 또는 성장 정체로 상쇄됩니다. 이로 인해 사례 건수가 너무 증가하여 이미 부하가 걸린 분석 팀에서 해결하기 힘든 경우, 부정 행위 팀은 **사례 마킹에 대한 피로감**을 겪을 수 있습니다. 이 경우 분석가가 어떤 사례가 가장 중요하고 어떻게 우선 순위를 결정해야 하는지 파악하기 어렵기 때문에 매우 위험합니다. 이러한 파악 능력이 부족하여 부정적인 활동을 방지하기 위해 신속하게 식별할 수 없는 경우, 이미 손실이 발생한 후에 부정 행위를 탐지하기 어려울 수 있습니다. 손실은 매우 클 수 있으며 보안 팀들은 공격의 특성, 공격에 대한 조직의 노출 수준, 전반적인 비즈니스에 미치는 영향에 대한 비즈니스 책임자들의 질문에 제대로 답하지 못할 수 있습니다.

조직과의 소비자 디지털 상호 작용이 증가함에 따라 조직의 매출을 늘릴 수 있는 기회가 생겨났지만, 이를 통해 잠재적인 침해 및 취약성도 증가합니다. 실시간으로 디지털 부정 행위 시도를 파악할 수 없는 경우 합법적인 사이트 사용자와 사이버 범죄자를 구분할 수 없기 때문에 오늘날의 조직에 큰 영향이 미칠 수 있으므로 이에 대한 적절한 계획이 필요합니다. 온라인 부정 행위는 브랜드 손상을 포함해 직접 및 간접적인 금융 손실을 일으켜 매년 수십억 달러의 매출 감소로 이어지며, 고객을 유치하고 유지할 수 있는 조직의 역량에 추가적인 영향을 미칩니다. 부정 행위자들은 승인되지 않은 계정을 열고 기존 계정의 소유권을 탈취하기 위해 더 많은 시도를 하고 있습니다.

따라서 조직은 실시간으로 부정 행위를 식별하는 기능과 부정 행위를 실시간으로 중단할 수 있는 제어 기능이 필요합니다. 계정 탈취 및 부정적인 자금 이동과 같은 악의적인 사용자 행동이 노출될 수 있도록 조직은 항상 사용자가 디지털 채널에서 수행하는 작업에 대해 포괄적으로 확인할 필요가 있습니다. 또한 위험 허용 한도, 리소스 및 전략적 우선 순위에 부합하는 방식으로 부정 행위 인시던트에 대응하는 능력도 필요합니다.

대부분의 조직은 대여섯 개의 독립적인 부정 행위 방지 툴을 사용해 각 툴이 특정 문제를 해결하도록 하지만, 이를 연결시키는 기능은 대부분 부족합니다. 조직이 전방위적 전략을 수행함에 따라 전체 채널에 대해 전반적인 부정 행위 탐지율을 개선하고 사례 관리를 중앙에 집중시키기 위해 여러 부정 행위 방지 툴에서 데이터를 연결시킬 필요성이 증가합니다.

지난 몇 년 동안 부정 행위는 주로 기술 문제로 여겨졌고, 부정 행위 방지 노력은 Cost Center로 여겨졌지만 이러한 인식은 빠르게 사라지고 있습니다. 조직은 이제 비즈니스 영향의 관점으로 부정 행위 방지 노력을 바라보고 있으며, 비즈니스 가치가 가장 높은 것에 대한 보안을 우선시 합니다. 이는 영업 매출 흐름을 보호하고 소비자에게 안전하고 원활한 디지털 경험을 제공하는 것을 포함합니다.

비즈니스 중심의 전방위적 부정 행위 관리 전략

기존의 부정 행위 방지 툴은 새롭게 발전하는 부정 행위 위협의 공격으로부터 조직을 적절히 보호할 수 없습니다. 기술 및 비즈니스 리더 간 파트너십의 강점을 활용하는 새로운 접근법이 필요한 때입니다.

비즈니스 중심의 전방위적 부정 행위 관리를 통해 디지털 채널 전반에 걸쳐 소비자 액세스 및 거래를 보호할 수 있는 계층화된 모델을 제공하고 이와 동시에 조직은 매출, 위험, 비용 및 소비자 편의성의 균형을 유지할 수 있습니다.

비즈니스 중심의 전방위적 부정 행위 관리 전략의 핵심은 원하는 비즈니스 성과를 정확하게 해석하는 것입니다. 부정 행위 및 보안 팀은 비즈니스 목표를 이해하고 각각의 결정을 원하는 비즈니스 성과에 맞춰야 합니다.

다이어그램 1: 전방위적 부정 행위 방지

매출 목표, 거래 포기율, 고객 개입, 부정 행위 탐지율 또는 부정 행위 예방처럼 간단한 KPI를 수립하는 것부터 시작합니다. 비즈니스 경영진이 이러한 KPI를 수립하면 부정 행위 관리 팀은 다음과 같은 방법으로 비즈니스 중심의 부정 행위 관리 전략을 구축하고 실행할 수 있습니다.

- **디지털 채널의 소비자 경험과 부정 행위로 인한 손실에 대한 위험 사이에 적절한 균형을 설정합니다.** 오늘날의 사용자는 디지털 채널에서 계정, 제품 및 서비스에 빠르고 쉽게 액세스하길 원하며 고객 경험이 중단되는 것을 원하지 않습니다. 성공적인 비즈니스 중심의 부정 행위 관리 전략은 조직의 보안 요구 사항과 편리한 사용자 액세스 및 마찰 없는 사용자 경험에 대한 필요와의 균형을 맞춰야 합니다.

- **적절한 소비자 인증 방법을 선택해야 합니다.** 이는 "모든 사항에 적합한 하나의 인증" 모델이 없기 때문에 매우 중요합니다. 조직은 다양한 디지털 채널에서 편리하게 사용할 수 있는 다양한 인증 방법을 제공해야 합니다. 기업은 거짓 양성이 낮고 거짓 음성도 낮은 정확한 방법을 찾아야 합니다. 이는 한 편으로는 소비자 경험, 다른 한 편으로는 부정 행위 방지율에 직접적인 영향을 미치기 때문입니다. 대부분의 최종 사용자에게 원활한 최종 사용자 경험을 제공하는 것이 고객 만족의 열쇠입니다. 소비자는 디바이스 종류, 시간에 관계없이 안전하고 편리한 방법으로 조직과 디지털 방식의 상호 작용을 원하므로 이러한 기대치를 충족하지 못하면 거래 포기율이 증가하거나 소비자를 경쟁업체에 잃게 되고 이는 조직의 매출 감소로 이어집니다.
- **소비자 디지털 상호 작용과 관련된 위험을 정확하게 진단합니다.** 이는 중단 없이 인증을 진행할 사용자와 추가 인증을 요청해야 하는 사용자를 결정하는 데 있어 매우 중요합니다. 이러한 목표를 달성하려면 부정 행위 탐지율이 높고 거짓 양성이 낮은 매우 정확한 위험 기반 인증 솔루션이 필수적입니다.
- **소비자가 모든 디지털 채널에서 상호 작용하는 방식에 대해 완벽하게 파악**하고 있는지 확인합니다. 이는 조직이 소비자가 상호 작용할 수 있는 디지털 채널을 더 많이 개설하려고 할 때 특히 중요합니다. 부정 행위자는 가장 취약한 링크를 찾고 보안 수준이 낮은 채널을 공격할 것입니다. 조직은 부정 행위자를 정상 사용자와 정확하게 구분할 수 있도록 소비자가 디지털 채널에서 하는 행동에 대해 파악하고 분석 정보를 제공하는 솔루션을 찾아야 합니다.
- 혼자서는 부정 행위에 맞서 싸울 수 없다는 사실을 직시해야 합니다. 성공적인 부정 행위 방지 및 완화를 위해 조직은 다른 조직과 유사한 특성으로 부정적인 공격을 방지하는 데 도움이 되는 **확인된 부정 행위에 대한 인텔리전스를 공유하고 협업**해야 합니다. 부정 행위에 맞서 싸우는 커뮤니티의 힘을 취합하면 부정 행위로 인한 손실을 크게 줄일 수 있습니다.

RSA의 비즈니스 중심 전방위적 부정 행위 관리 솔루션

RSA Fraud & Risk Intelligence Suite는 부정 행위 예방 노력을 위험 허용 한도 및 전략적 우선 순위에 맞춰 고객 기반이 아닌 부정 행위를 줄이려는 조직을 위해 설계되었습니다. 이 제품군은 위험 기반 의사 결정, 예측 분석, 심층적인 엔티티 프로파일링, 유연한 규칙 기반 정책 관리 및 공유된 글로벌 부정 행위 인텔리전스를 결합한 중앙 집중식 부정 행위 탐지 및 완화 전략을 통해 디지털 채널 전체에 걸쳐 통합적인 관점을 제공하며, 기타 부정 행위 방지 툴에서 얻은 분석 정보를 통합해 부정 행위 위험 진단을 강화하고 타겟 사이버 범죄 공격에 대해 고객을 더 효과적으로 보호합니다.

이 제품군은 최종 사용자와 디지털 채널 간의 상호 작용을 분석하여 숨은 부정 행위를 밝혀냅니다. 또한 RSA Fraud & Risk Intelligence Suite는 로그인 및 거래와 같은 세션 중 주요 지점에서 위험 기반 의사 결정을 지원합니다. 자가 학습형 위험 진단 엔진은 심층적인 엔티티 프로파일링을 수행하고, 부정 행위자가 특정 행동을 수행했을 가능성을 반영하는 위험 수치를 계산합니다.

RSA Fraud and Risk Intelligence Suite는 소비자 디지털 여정의 모든 단계를 보호합니다.

- **RSA FraudAction™**은 공격 진압 및 사이버 인텔리전스를 제공하는 단일 외부 위협 관리 서비스입니다. 탐지부터 신속한 차단에 이르기까지 RSA FraudAction 360은 피싱 공격, 트로이 목마 공격, 악성 모바일 애플리케이션 및 악성 소셜 미디어 페이지에 대한 완전한 적용 범위를 제공합니다. FraudAction Cyber Intelligence Service는 브랜드와 관련된 사이버 범죄 환경 및 운영에 대한 폭넓게 파악할 수 있는 능력을 제공하며, 소셜 미디어 포럼 내에서의 심층 연구와 함께 다크 웹에 대한 깊고 오랜 파악 능력을 활용합니다.
- **RSA Adaptive Authentication**은 디지털 채널 전반에서 소비자를 부정 행위로부터 보호하려는 조직에 위험 기반 다단계 인증을 제공하는 전방위적 고급 부정 행위 탐지 허브입니다. RSA Risk Engine으로 작동하는 RSA Adaptive Authentication은 다양한 위험 지표를 평가하여 사용자의 로그인 및 로그인 후 활동과 관련된 위험을 측정하도록 설계되었습니다. 강력한 머신 러닝과 함께 세분화된 정책 제어 옵션을 사용하는 RSA Adaptive Authentication은 위험도가 높은 시나리오 및 조직이 수립한 규칙을 위반한 시나리오에 대해 아웃오브밴드 인증과 같은 추가 보증만을 요구하는 부정 행위 방지 허브입니다. 이 방법은 작업에 영향을 미치지 않는 인증을 통해 대부분의 사용자에게 원활한 최종 사용자 경험과 높은 부정 행위 탐지율을 제공합니다.
- **RSA Adaptive Authentication for eCommerce**는 신용 카드 발급사를 위한 RSA의 EMV 3-D Secure 솔루션입니다. 3-D Secure 프로토콜과 인프라스트럭처, Adaptive Authentication for eCommerce를 활용하여 차지백 손실의 위험을 완화하면서 판매업체와 카드 발급사가 카드 소유자에게 일관성 있고 안전한 온라인 쇼핑 환경을 제공할 수 있도록 합니다. RSA의 Risk Engine을 기반으로 하는 RSA Adaptive Authentication for eCommerce는 선한 카드 소지자를 자동으로 인증하고 위험도가 높은 소수의 최종 사용자에게만 확인을 진행하여 원활한 쇼핑 경험을 제공합니다. 선한 고객에게 원활한 쇼핑 경험을 제공하는 동시에 정확하게 본인 확인을 진행하고 부정 행위를 제거하는 능력은 업계 내에서 타의 추종을 불허합니다.

다이어그램 2: RSA Fraud & Risk Intelligence Suite - 디지털 소비자 수명주기 보호

검증된 소비자 부정 행위 방지

- 20억 명 이상의 소비자 보호
- 1년에 40억 달러 이상의 부정 행위로 인한 손실 방지
- 1백만 건 이상의 사이버 공격 차단
- 3~5%의 개입률만으로 95% 이상의 부정 행위 탐지율

부정 행위에 함께 맞서 싸우는 커뮤니티인 RSA eFraudNetwork에 매일 기여하는 수천 명의 직접 및 간접 고객

RSA Fraud & Risk Intelligence Suite는 분산된 기능과 데이터 소스를 통합하여 개별 사용자 활동과 행동에 대한 포괄적인 관점을 제공합니다. 이러한 제품 간 교류를 통해 더 정확한 부정 행위 탐지를 제공하고 조직의 위험 허용 한도 및 전략적 우선 순위에 맞게 매우 세분화되고 개인화된 부정 행위 방지 전략을 만드는 역량을 제공합니다.

RSA Fraud & Risk Intelligence Suite의 솔루션에는 다음과 같은 다양한 통합 포인트가 있습니다.

- **RSA eFraudNetwork™**는 확인된 부정 행위 데이터 요소에 대해 RSA Fraud & Risk Intelligence 고객 커뮤니티 간에 공유되는 세계 최초이자 최대 규모의 저장소입니다. eFraudNetwork에서 공유되는 데이터를 활용하여 고객은 동료들이 공유하는 확인된 부정 행위를 기반으로 새로운 유형의 부정적인 활동을 신속하게 발견하고 조직의 환경에 대한 부정 행위를 예방할 수 있습니다.
- **RSA Adaptive Authentication Eco System 접근 방식**은 다양한 소스의 데이터 요소를 사용하여 부정 행위 탐지 기능을 향상시키도록 설계되었습니다. 타사의 정보를 사용하여 위험 진단 및 위험 수치에 영향을 미치므로 고객은 내부 비즈니스 인텔리전스 및 추가 부정 행위 방지 툴에서 추가적인 분석 정보를 제공할 수 있습니다. 오늘날, 조직의 50% 이상이 부정 행위 예방 작업에 4개에서 10개 가량의 서로 다른 부정 행위 방지 툴을 사용하고 있습니다. Adaptive Authentication Eco System 접근 방식을 활용하면 조직은 다양한 부정 행위 방지 툴에 대한 기존 투자를 활용하면서 Adaptive Authentication의 위험 진단 및 사례 관리를 중앙으로 집중시켜 운영 비용을 절감하고 부정 행위 탐지를 증가시킬 수 있습니다.

통합 RSA Fraud & Risk Intelligence 솔루션을 활용하면 조직의 디지털 채널에 더 나은 파악 기능을 제공하여 조직이 더 빠르고 효율적으로 부정 행위를 탐지하고 완화할 수 있도록 지원합니다.

RSA Fraud & Risk Intelligence Suite는 종합적이고 전방위적인 부정 행위 탐지 및 완화 기능을 제공하므로, 이를 통해 조직은 혁신적인 변화와 편의에 대해 증가하는 소비자의 요구를 충족할 수 있으며 이와 동시에 부정 행위로 인한 손실과 운영 비용을 절감할 수 있습니다.

부정 행위 방지에 대한 비즈니스 중심 접근 방식을 통해 부정 행위 방지 책임자는 부정 행위 위험에 대한 현재 비즈니스에 미치는 영향을 논의하고, 비즈니스 경영진과 협업하여 고객이 아닌 부정 행위를 중단하는 등 조직에서 가장 중요한 것을 보호하도록 하여 미래에 대비하는 준비를 갖출 수 있습니다.

디지털 위험은 모두에게 중요한 과제이며, 이 위험을 관리하도록 지원하는 것은 RSA의 몫입니다.

RSA의 비즈니스 중심 보안 제품 및 서비스는 통합 파악 능력, 자동화된 분석 정보 및 조율된 작업에 따라 디지털 위험을 관리하는 통합된 접근 방식을 조직에 제공합니다. RSA를 통해 지능형 공격을 효과적으로 탐지 및 대응하고 사용자 액세스 제어를 관리하며, 비즈니스 위험 요소, 부정 행위 및 사이버 범죄를 최소화할 수 있습니다. RSA는 전 세계 수백만 명의 사용자를 보호하고, Fortune지 선정 500대 기업의 90%가 넘는 기업이 성장하고 혁신 변화에 지속적으로 적응할 수 있도록 지원합니다.

역동적이고 위험도 높은 디지털 세상에서 성공하는 방법을 rsa.com/ko-kr에서 확인하십시오.