RSA

ソリューション概要

コンシューマー向けデジタル チャネルにおけるリスク管理

RSA FRAUD & RISK INTELLIGENCE SUITE

概要

コンシューマーの世界は、これまで経験していたよりも多くの方法で人々が連携や取引を行っているため、歴史的な転換点を迎えています。組織ではデジタル トランスフォーメーションが進行しており、利便性を求める消費者の声に応えるために、ますます多くのデジタル チャネルを消費者に公開しています。その結果、組織は、かつてないビジネスとセキュリティのリスクに直面しています。これは、法律によるプレッシャーから、新規参入企業との競争、不正行為者やサイバー犯罪者によって悪用される可能性のある潜在的な脆弱性の増大にまでわたっています。

消費者空間におけるこれらの変化は、医療機関、保険会社、加盟店までさまざまなタイプの組織に影響を与えています。そして特に、金融機関は次のような大規模な混乱に直面しています。

- **利便性とスピードに対するお客様の期待が高まっている**：お客様は、いつでも、どのデバイスからでも情報にアクセスでき、デジタル取引を高速かつ円滑で、パーソナライズされ、チャネルに依存しない、安全な方法で実行できることを期待しています。
- FinTech**のイノベーション**は、デジタル サービスを提供する新しい競争につながっており、組織は自社の戦略を再検討し、APIエコノミーを活用した新しいパートナーシップを構築することを余儀なくされています。それだけでなく、管理する必要のあるサードパーティーのリスクももたらしています。
- **世界的な規制の広がり**により、PSD2、GDPR、SEPA、FFIECなどの消費者データ保護、セキュリティ、プライバシーに対するアカウンタビリティが高まっています。
- **支払いの革新**は、デジタル決済量の大幅な増加を促しています。その中で、EMV 3D-Secureは3DSエコシステムを通じて加盟店のトラフィックの増加を推進すると予想されています。3DSエコシステムには、「Faster Payments」（世界中でさまざまな形態や形式がある）、クラウド決済アプリケーション、その他のFinTechアプリケーションなどがあります。そのため、デジタル チャネルを介して送金される金額の合計が増加し、不正による損失が増加する危険にさらされています。

RSA FRAUD & RISK INTELLIGENCE SUITE

- *何の不便もなく**自信を抱かせる***
- *お客様や収益ではなく**不正を削減する***
- *あらゆるデジタル対話の**リスクを明らかにする***
- *総合的なインテリジェンスを使用して**洞察を最適化する***
- *不正操作の**効率を向上させる***
- ***サイバー犯罪を凌ぐ***

- Internet of Things（IoT）により、さまざまなデバイスが消費者に代わってさまざまなアクティビティを実行できるようになります（その一例は、Alexaです）。その結果、アカウント所有者のIDは実質的に使用されなくなりますが、組織は正規のデジタル対話を不正な対話から区別できる必要があります。
- 組織が**オムニチャネル戦略**を開始するにつれて、セキュリティ侵害と脆弱性の潜在的なポイントの拡大が続いています。新しいチャネルが追加されるたびに、効率性が向上し、財務へのアクセスが合理化されますが、その反面、セキュリティの脆弱性も生じます。
- **デジタル アクティビティと取引量の大幅な増加**は、不正を軽減および調査する組織リソースの増加が最小（またはなし）であることで相殺されます。これで、すでに圧倒されているアナリスト チームが対処できないほどにケースの負荷が膨大になりすぎると、不正チームは**ケースの格付けに疲労**してしまう可能性があります。アナリストはどのケースが最も重要で、何が優先されるべきかを理解するのに苦労するため、これは危険な結果を招きます。このように可視性が欠如していると、不正行為をすばやく特定して阻止することができないため、損失が発生した後も不正に気付かない恐れがあります。そうなると、損失は膨大なものになる可能性があります。また、セキュリティ チームは、攻撃の性質、組織がどの程度攻撃を受けたか、全体的なビジネスへの影響などの質問をビジネス リーダーに尋ねられても答えられないことに気付く場合があります。

組織と消費者とのデジタル対話が増加していることは、組織の収益を拡大する機会をもたらしますが、同時にセキュリティ侵害や脆弱性の潜在的なポイントも増えることになります。デジタル不正の試行をリアルタイムで識別できないこと、つまり正規のサイト ユーザーとサイバー犯罪者を区別できないということは、今日の組織に大きな結果をもたらす可能性があります。したがって、適切な計画が必要になります。オンライン詐欺は、ブランドの損害を含む直接的および間接的な経済的損失の観点からは、年間数十億ドルの減益をもたらします。これは、組織がお客様を引き付けて、保持できるかどうかという点にも影響を及ぼします。犯罪者が不正なアカウントを開き、既存のアカウントの所有権を取得しようとする不正行為が増えています。

その結果、組織は不正をリアルタイムで特定する能力と、不正をリアルタイムで阻止するための制御を必要としています。アカウントの乗っ取りや不正な送金など、悪意のあるユーザーの行動が明らかになるように、組織はユーザーがデジタル チャネルで実行している処理をいつでも包括的に把握する必要があります。ただし、リスク許容度、リソース、戦略的な優先順位と調和した方法で、不正インシデントに対応する能力も必要です。

ほとんどの組織は、五指に余るほどの独立した不正防止ツールを利用して、それぞれ特定の問題を解決しているにもかかわらず、多くの組織は問題を関連付けることができません。組織がオムニチャネル戦略を実行するようになって初めて、すべてのチャネルにわたる全体的な不正検出率を向上させ、ケース管理を一元化するために、さまざまな不正防止ツールからのデータを関連付ける必要が大きくなります。

過去何年もの間、不正は主にテクノロジーの問題と見なされ、不正防止対策は原価部門の担当と見なされていましたが、そうした時代は急速に過ぎ去ろうとしています。組織は現在、ビジネスへの影響という観点から不正防止対策を行っており、ビジネスはセキュリティを最優先させるようになっています。これには、営業収益の流れを保護し、消費者に安全で円滑なデジタル体験を提供することが含まれます。

ビジネス主導のオムニチャネル詐欺管理戦略

従来の不正対策ツールでは、新たに進化した不正の脅威から組織を適切に保護することはできません。テクニカル リーダーとビジネス リーダー間のパートナーシップの強みを活用した新しいアプローチを採用するのは今です。

ビジネス主導型のオムニチャネル不正管理は、収益、リスク、コスト、消費者の利便性のバランスを取りながら、デジタル チャネル全体で消費者のアクセスと取引を保護するための階層化されたモデルを提供します。

ビジネス主導のオムニチャネル不正管理戦略の中核となるのは、予期されたビジネス上の成果を正確に変換することです。不正チームとセキュリティ チームはビジネス目標を理解する必要があり、それぞれの意思決定は予期されたビジネス上の成果と一致する必要があります。

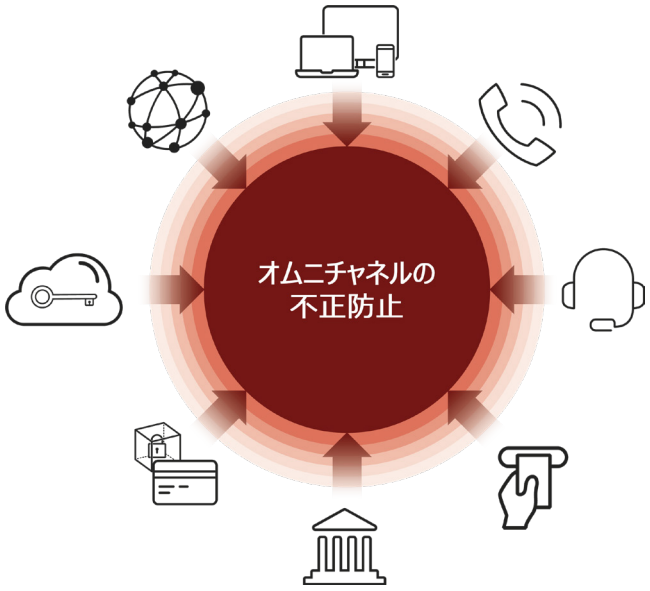

図1：オムニチャネルの不正防止

出発点は、収益目標、取引放棄率、お客様の介入、不正検出率、不正損失防止などの単純なKPIを確立するです。これらのKPIがビジネス リーダーシップによって確立された場合、不正管理チームは次の方法でビジネス主導の不正管理戦略を構築および実行できます。

- **デジタル チャネルにおける消費者のエクスペリエンスと不正による損失のリスクとの適切なバランスを設定します。**今日のユーザーは、デジタル チャネルでアカウント、製品、サービスにすばやく簡単にアクセスできることを求めており、エクスペリエンスが中断されることを望みません。ビジネス主導の不正管理戦略を成功させるには、組織のセキュリティ要件と、ユーザー アクセスの利便性や円滑なユーザー エクスペリエンスの必要性のバランスをとる必要があります。

- **適切な消費者認証方法を選択します。**「1つの認証ですべてに対応する」モデルはないため、このことも重要になる可能性があります。組織は、さまざまなデジタル チャネルで使用する便利な認証方法を何種類か用意する必要があります。これは、一方で消費者のエクスペリエンスに、他方では不正防止率に直接的な影響を及ぼすため、低偽陽性と低偽陰性を含め、正確な方法を模索する必要があります。組織のエンド ユーザーの大多数に円滑なエンド ユーザー エクスペリエンスを提供することは、顧客満足度を高めるための鍵です。消費者は、安全かつ便利な方法で、いつでもどのデバイスからでも組織とデジタル的に対話できることを期待しているため、これらの期待に応えることができないと、取引放棄率が増加したり、競合他社にお客様を奪われたりする可能性があります。それは組織の減益につながります。
- **消費者のデジタル対話に関連するリスクを正確に評価します。**これは、透過的に認証できるユーザーと、追加認証を求めるユーザーを決定するために重要です。この目標を達成するには、不正検出率が高く、偽陽性が少ない、非常に正確なリスクベースの認証ソリューションが不可欠です。
- **消費者がすべてのデジタル チャネルで対話している方法を完全に把握している**ことを確認します。組織は消費者が対話に使用するデジタル チャネルをさらに開こうとしている場合には、特に重要です。犯罪者は最も脆弱なリンクを探し、安全性の低いチャネルを攻撃します。組織は、犯罪者と正規ユーザーを正確に区別できるようにするために、消費者がデジタル チャネルでどのように行動しているかを可視化し、洞察を提供するソリューションを探す必要があります。
- 組織は一人で不正と戦うことができないことを認識します。不正の防止と軽減を成功させるために、組織は**連携して、確認された不正行為に関する情報を共有する**必要があります。これは、他の組織で類似した特徴を持つ不正な攻撃を防ぐのに役立ちます。コミュニティーが団結して不正に対抗すれば、不正による損失を大幅に減らすことができます。

RSAのビジネス主導のオムニチャネル不正管理ソリューション

RSA Fraud & Risk Intelligence Suiteは、お客様ベースではなく不正を削減できるように、不正防止対策をリスク許容度と戦略的な優先事項に合わせて調整しようとしている組織を対象としています。このスイートは、リスクベースの決定、予測分析、ディープ エンティティ プロファイリング、柔軟なルールベースのポリシー管理、共有されたグローバルな不正インテリジェンスを独自に融合した、一元化された不正検出および緩和戦略により、デジタル チャネル全体の包括的なビューを提供します。また、他の不正防止ツールからの洞察を組み込んで不正リスク評価を補強し、標的型サイバー犯罪攻撃からお客様をより適切に保護することができます。

このスイートは、エンド ユーザーとデジタル チャネルの間の各操作を分析することによって、そうでなければ見逃されてしまう不正を明らかにします。さらに、RSA Fraud & Risk Intelligence Suiteは、ログインや取引などのセッション中の重要なポイントにおいて、リスクベースの決定をサポートします。自己学習型リスク エンジンは、ディープ エンティティ プロファイリングを実行し、犯罪者によってアクティビティが実行される確率を反映したリスク スコアを計算します。

RSA Fraud and Risk Intelligence Suiteは、消費者のデジタル化のすべてのステップを保護します。

- RSA FraudAction™は、攻撃の排除とサイバー インテリジェンスを提供する単一の外部脅威管理サービスです。RSA FraudAction 360は、検出から迅速なシャットダウンまで、フィッシング攻撃、トロイの木馬攻撃、不正なモバイル アプリ、不正なソーシャル メディア ページに完全に対応します。FraudAction Cyber Intelligence Serviceは、ダーク ウェブに対する長年にわたる詳細な可視性を、ソーシャル メディア フォーラム内での詳細な調査と組み合わせて活用し、ブランドに関連するサイバー犯罪の状況と実施を広範囲に可視化します。
- RSA Adaptive Authenticationは、高度なオムニチャネル不正検出ハブであり、デジタル チャネル全体で不正から消費者を保護しようとする組織にリスクベースの多要素認証を提供します。 RSAリスク エンジンを搭載したAdaptive Authenticationは、さまざまなリスク インジケーターを評価することで、ユーザーのログインおよびログイン後のアクティビティのリスクを測定できるように設計されています。RSA Adaptive Authenticationの不正防止ハブは、強力な機械学習ときめ細かいポリシー制御のオプションを使用して、リスクが高い場合や、組織が確立したルールに違反している場合に限り、帯域外認証などの追加保証を必要とします。この方法では、大多数のユーザーに透過的な認証を提供して、円滑なエンド ユーザー エクスペリエンスと高い不正検出率を保証します。
- RSA Adaptive Authentication for eCommerceは、クレジット カード発行会社や発行側の決済処理業者向けの、RSAのEMV 3-Dセキュア ソリューションです。Adaptive Authentication for eCommerceは、3Dセキュア プロトコルとインフラストラクチャを利用して、加盟店やカード発行会社がチャージバックによる損失のリスクを軽減しながら、カード所有者に一貫した安全なオンライン ショッピング体験を実現します。RSAのリスク エンジンを搭載したRSA Adaptive Authentication for eCommerceは、優良のカード所有者を暗黙的に認証し、少数のリスクの高いエンド ユーザーにのみチャレンジすることにより、円滑なショッピング体験を提供します。優良なお客様に円滑なショッピング体験を提供しながら、正確にチャレンジして不正を排除できる能力は、業界で卓越しています。

図2：RSA Fraud & Risk Intelligence Suite - デジタル消費者のライフサイクルを保護

実証された消費者不正防止

- ***20億以上**の消費者を保護*
- *1年で**40億ドル以上**の不正による損失を阻止*
- ***100万以上**のサイバー攻撃を遮断*
- ***95%以上の不正検出**率（介入率は**3～5%**のみ）*

***何千もの**直接的または間接的なお客様が**RSA eFraudNetwork**に毎日**貢献**し、コミュニティーとして不正に対抗*

RSA Fraud & Risk Intelligence Suiteは、サイロ化された機能とデータ ソースを統合して、個々のユーザー アクティビティと行動を総合的に把握します。この製品間の融合によって、不正検出の精度が高く、組織のリスク許容度と戦略的な優先順位に調和した、非常にきめ細かい、パーソナライズされた不正防止戦略を作成することができます。

RSA Fraud & Risk Intelligence Suiteのソリューションには、次のような多数の統合ポイントがあります。

- RSA eFraudNetwork™：RSA Fraud & Risk Intelligenceのお客様のコミュニティー間で共有される、確認済みの不正データ要素から成る世界初かつ最大のリポジトリー。お客様はeFraudNetwork内で共有されたデータを活用して、同業他社が共有している確認済みの不正に基づいて、新しいタイプの不正アクティビティをすばやく発見し、環境内での不正を防止できます。
- RSA Adaptive Authentication Eco System**アプローチ**は、さまざまなソースからのデータ要素を使用して、不正検出を強化するように設計されています。お客様は、リスク アセスメントに影響を与え、リスク スコアに反映するために、サード パーティーのファクトを利用できます。そのようにして、社内のビジネス インテリジェンスと追加の不正防止ツールの両方からさらに洞察を提供することができます。最近では、50%以上の組織が、不正行為防止のために4～10種類の不正防止ツールを利用しています。Adaptive Authentication Eco Systemアプローチを活用することで、組織はさまざまな不正防止ツールに対する既存の投資を活用しながら、Adaptive Authenticationのリスク アセスメントとケース管理を一元化して、運用コストの削減と不正検出率の向上を達成することができます。

統合されたRSA Fraud & Risk Intelligenceソリューションを活用すると、組織のデジタル チャネルの可視性が向上し、不正をより迅速かつ効率的に検出して軽減することができます。

RSA Fraud & Risk Intelligence Suiteは、全体的なオムニチャネル不正検出機能と軽減機能を提供するため、組織は変革による変化や消費者による利便性の向上を求める声に継続的に適応しながら、不正による損失と運用コストを削減できます。

不正防止へのビジネス主導のアプローチにより、不正防止リーダーは不正によるリスクが現在のビジネスに与える影響を議論し、ビジネス リーダーとさらに連携して将来に備える態勢を適切に整えています。それは、組織にとって最も重要なことを保護する、つまりお客様ではなく不正を阻止することによって可能になります。

誰もが持つデジタル リスクの管理を
RSAがサポート

RSAはビジネス主導型のセキュリティ製品とサービスを提供し、さまざまな組織が、統合的な可視性、自動化されたインサイト、および組織的なアクションを使用してデジタル リスク管理のための統合的なアプローチを採用できるようサポートしています。RSAは、高度な攻撃の効果的な検出と対応、ユーザー アクセス制御の管理、さらにビジネス リスク、不正行為、サイバー犯罪の削減を支援できます。RSAは、世界中の数百万人のユーザーを保護し、Fortune 500の企業の90%以上が成功し、革新的な変化に継続的に適応できるように支援しています。

リスクの高い動的なデジタルの世界で成功を収める方法については、rsa.com/ja-jpをご覧ください。