Estudo de Caso

Detecção de vivacidade e biometria móvel

Como os bancos latino-americanos usam a Knomi™ para conquistar mais clientes e evitar fraudes

AWARE

Introdução

Para os clientes de bancos da Aware na região, a biometria e o reconhecimento facial em particular estão desempenhando um papel importante ao tornar as operações bancárias mais acessíveis, práticas e seguras.

Os avanços significativos da tecnologia e das redes de telefonia móvel oferecem aos bancos a oportunidade de tornar seus serviços mais acessíveis. Agora os clientes podem usar seus dispositivos móveis para solicitar rapidamente novas contas e linhas de crédito, acessar as informações da conta e realizar compras e transações, tudo sem precisar visitar uma agência ou caixa eletrônico. O crédito para a compra de itens caros, como eletrodomésticos, eletrônicos e móveis, pode ser emitido no local pelos varejistas no momento da compra.

Por muitas medidas, a América Latina lidera o mundo na adoção da biometria para aplicações comerciais, e as empresas de serviços financeiros são os que mais contribuem para a tendência. Para os clientes de bancos da Aware na região, a biometria e o reconhecimento facial em particular estão desempenhando um papel importante ao tornar as operações bancárias mais acessíveis, práticas e seguras.

Em todos os casos, os bancos estão usando a "detecção de vivacidade" oferecida como parte da solução de autenticação biométrica móvel Knomi™ da Aware. A detecção de vivacidade é usada para garantir que as imagens faciais sendo coletadas sejam confiáveis para várias verificações de segurança baseadas em biometria. É aplicada durante a integração de novos clientes e para o login aprimorado em aplicativos móveis usando autenticação biométrica.

Exemplos de fraudes evitadas por reconhecimento de íris e detecção de vivacidade

Os bancos na América Latina estão muito familiarizados com as diversas formas de fraudes utilizadas para tentar roubar dos bancos e dos clientes. Entre elas estão os "ataques de apresentação" que tentam derrotar os mecanismos de segurança biométricos. Em alguns dos casos mais comuns, a fraude é perpetrada não por estranhos, mas por membros da família e até mesmo por funcionários. Os fraudadores profissionais tendem a confiar em técnicas mais repetíveis. Em ambos os casos, a biometria torna a integração e a autenticação mais resiliente a fraudes, mas requer detecção de vivacidade para isso. A seguir estão alguns exemplos de ataques de apresentação e o papel da detecção de vivacidade.

ATAQUES INTERNOS

Uma categoria comum de fraude é cometida por uma parte conhecida: um membro da família, amigo ou colega de trabalho com acesso relativamente fácil aos dados de identidade de seu alvo inocente. Eles tentam se passar pela vítima, abrir uma nova conta em seu nome ou acessar a conta existente sem o conhecimento da vítima. O uso do reconhecimento facial e da biometria de voz torna esses tipos de ataque muito mais difíceis. Em ambos os casos, a detecção de vivacidade é necessária para impedir que o perpetrador use uma foto ou um vídeo de sua vítima (uma "falsificação") para representá-la.

Uma categoria menos comum de fraude interna é cometida por funcionários do banco. Nesse caso, um funcionário coleta dados de identidade de um solicitante de conta como parte de seu processo de integração, mas também tira uma foto ou vídeo do cliente usando seu dispositivo móvel pessoal. O candidato não percebe que isso não faz parte do processo padrão. O funcionário usa as informações da conta e a imagem facial do cliente para acessar a nova conta. A linha de crédito do cliente desaparece antes que ele possa usá-la. A detecção de vivacidade impede esse tipo de ataque interno.

IDENTIDADES SINTÉTICAS

Outra categoria de fraude envolve a criação de "identidades sintéticas" que são criadas e usadas pelos fraudadores para obter crédito e

empréstimos que eles não planejam pagar. Os fraudadores podem fazer isso repetidamente usando conjuntos de informações de identidade que são completamente fictícias ou baseadas parcialmente em uma pessoa real. A biometria facial pode ser usada para ajudar a proteger um processo móvel de integração contra o uso de identidades sintéticas. Mas, sem a detecção de vivacidade, um fraudador pode usar uma foto ou um vídeo de outra pessoa ou ainda uma selfie em que seu rosto está parcialmente obscuro. Isso evita que a imagem seja usada para vários mecanismos de segurança biométricos de integração úteis (veja abaixo).

Como os bancos latino-americanos usam a Knomi para a integração segura e de baixo atrito

Os novos clientes são uma fonte crítica do crescimento da receita de qualquer banco, portanto, integrá-los com eficiência está entre as funções mais importantes a serem executadas. Mas a integração também é o momento em que os bancos ficam mais vulneráveis à fraude. A integração é em grande parte um exercício de verificação de identidade, onde o banco tenta avaliar se um possível titular de conta pode ser confiável com uma linha de crédito e se comportará como um cliente de boa-fé.

Os bancos que incorporaram o software da Knomi em seu processo de integração podem usar uma selfie em tempo real do solicitante para realizar várias verificações de identidade que servem para verificar positivamente sua identidade e detectar uma tentativa de fraude.

Diferentes versões da Knomi permitem que o processo seja conduzido a

Os novos clientes são uma fonte crítica do crescimento da receita de qualquer banco, portanto, integrá-los com eficiência está entre as funções mais importantes a serem executadas.

partir do aplicativo móvel do banco ou, alternativamente, por meio de uma página da Web em um dispositivo móvel ou desktop. Um URL pode ser descoberto pelo solicitante no site do banco, no email de anúncio ou no banner. Basta que um cliente potencial clique no link em seu celular ou desktop para iniciar um processo de solicitação em um navegador, o que inclui a captura de uma selfie em tempo real. Dessa forma, um processo baseado em navegador e aprimorado com biometria pode aumentar a segurança e simultaneamente reduzir o atrito de um processo de integração que não exige que o solicitante instale um aplicativo móvel antes da solicitação.

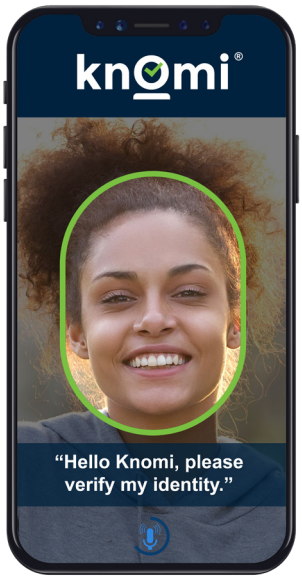
Os bancos latino-americanos estão usando o reconhecimento facial e a detecção de vivacidade da Knomi para conduzir diferentes verificações de identidade e de detecção de fraude no momento da integração. Por si só, a detecção de vivacidade já serve a vários propósitos valiosos:

- **Detecção de tentativas de representação de uma vítima visada usando "falsificações"**, como fotos em papel ou digitais, vídeos ou máscaras 2D e 3D;
- **Detecção de tentativa de ocultação de identidade usando uma imagem facial não própria**, não humana ou parcialmente obscurecida para evitar detecção por pesquisas baseadas em reconhecimento facial no futuro; e
- **Não repúdio**, um termo que descreve a capacidade de um banco coletar evidências admissíveis em tribunal para associar a atividade de um fraudador a uma pessoa real, ou seja, impedir que o fraudador repudie seu envolvimento em uma tentativa de fraude.
- **Mas a detecção de vivacidade também é uma parte essencial dessas outras medidas de segurança que dependem da correspondência e da pesquisa biométrica**, cada qual sendo empregada por um ou mais clientes latino-americanos da Aware como parte de um processo de integração:
- **Correspondência de identificação a imagem facial.** Essa função, juntamente com a detecção de vivacidade, garante que o documento de identidade emitido pelo governo e usado para transmitir dados de identificação seja autêntico e pertença ao solicitante.
- **Verificações de duplicatas.** As imagens faciais de outros clientes são pesquisadas para garantir que o solicitante não esteja tentando manter várias contas clandestinamente, usando uma identidade sintética ou assumindo a identidade de um titular de conta existente.
- **Verificações da lista de observação.** São realizadas pesquisas em bancos de dados de imagens faciais de fraudadores conhecidos para garantir que o solicitante não seja um deles.

- **Verificações de agências externas.** Imagens faciais podem ser enviadas a agências de aplicação da lei externas para determinar se o indivíduo em questão tem antecedentes criminais.

Autenticação móvel usando biometria confiável da integração

Depois que os clientes são integrados e abrem uma conta, os bancos podem usar a selfie capturada durante o processo de cadastro para permitir o acesso à conta de forma mais segura e prática e a realização de transações por meio do aplicativo móvel. Os clientes latino-americanos da Aware incorporaram a autenticação biométrica a seus aplicativos de banco móvel, onde é usada como uma alternativa às senhas ou como uma etapa necessária além das senhas para transações de maior valor.



Como a integração, a detecção de vivacidade é uma função essencial da autenticação biométrica móvel, pois sem ela um fraudador com acesso ao telefone da vítima poderia usar uma falsificação para representar o proprietário do dispositivo e acessar suas contas. A detecção de vivacidade impede esse ataque de apresentação.

Outra maneira de tornar a autenticação biométrica ainda mais resistente à falsificação é empregando uma abordagem multimodal, ou seja, exigindo uma modalidade biométrica além da face, como a voz. Isso melhora o desempenho da segurança biométrica (menos correspondências falsas) e a praticidade (menos não correspondências falsas) por ordem de magnitude.

Porém, adicionar correspondência de voz e detecção de vivacidade também torna a tarefa de falsificar exponencialmente mais complicada. A detecção de vivacidade da voz utiliza algoritmos que detectam se uma amostra de voz foi gravada anteriormente ou gerada sinteticamente. Com uma abordagem apenas de rosto, o fraudador precisa de uma falsificação de rosto bem feita para derrotar a segurança biométrica. Com o rosto e a voz juntos, o fraudador também precisa corresponder e falsificar com sucesso a voz da vítima, o que é particularmente difícil, em parte porque amostras de voz que poderiam ser usadas para criar uma falsificação são muito mais difíceis de encontrar. Em suma, a biometria multimodal tem um efeito exponencial no desempenho e na segurança, o que é muito útil para transações de alto valor.

Adicionar correspondência de voz e detecção de vivacidade também torna a tarefa de falsificar exponencialmente mais complicada.

A biometria está se tornando uma parte essencial das operações bancárias móveis

As expectativas dos consumidores de seus aplicativos de banco móvel continuam aumentando, principalmente à medida que usamos menos dinheiro vivo. No entanto, não há expectativas de que essa capacidade venha com qualquer sacrifício em relação à segurança. A identidade é um elemento fundamental do sistema bancário e a biometria é uma abordagem de verificação de identidade poderosa e elegante, complementar a outros mecanismos de segurança. A biometria também oferece um nível de praticidade desejado pelos consumidores. Para vários bancos da América Latina, a biometria é essencial para os negócios. Eles veem a biometria como uma característica fundamental de seus serviços e marca. Com a Knomi, a Aware os ajuda a transformar essa visão em realidade.