White Paper

Melhorando o onboarding digital e a autenticação de usuários de aplicativos financeiros por meio da biometria

AWARE

781.687.0300 | sales@aware.com | www.aware.com

A Aware é uma empresa líder global de produtos de software e soluções para identificação e autenticação biométrica. Os mesmos são utilizados em uma variedade de aplicações, incluindo serviços financeiros, segurança empresarial, gestão de fronteiras e segurança pública. A Aware é uma empresa de capital aberto (NASDAQ: AWRE) com sede em Burlington, Massachusetts.

O mundo realmente se tornou digital. Atualmente, estima-se que 3,8 bilhões de pessoas possuam um smartphone1, o que representa quase metade de toda a população mundial. O rápido crescimento e adoção de smartphones em todo o mundo nos últimos anos mudou muito a forma como vivemos nossas vidas, das mídias sociais às compras online. Bancos e empresas de serviços financeiros também tiveram que se adaptar a esse novo cenário digital, oferecendo a seus clientes novas formas de acessar e gerenciar suas contas.

A chegada do COVID-19 apenas acelerou essas tendências, aumentando muito a demanda geral por soluções financeiras baseadas em plataformas digitais que não exigissem visitas que pudessem colocar a saúde em risco. Essa combinação de onipresença de smartphones e limitação de locomoção colocou em cheque os procedimentos de onboarding e autenticação de usuários tradicionais, destacando o quão importante é fornecer aos clientes um meio para abrir e acessar suas contas remotamente com segurança. Com tantos bancos e empresas financeiras procurando maneiras de enfrentar esses desafios, a biometria é a solução ideal para o cadastramento remoto (onboarding) e a autenticação segura de usuários e transações.

A Oportunidade do Banco Digital

Para as instituições financeiras, o mobile banking tornou-se uma forma econômica de alcançar novos clientes. A Tecnologica permite o acesso do cliente a contas financeiras de praticamente qualquer lugar do mundo, transações financeiras em tempo real sem visitar uma filial e conveniência sem precedentes em geral. Os clientes tem reagido bem às soluções móveis, com 47% dos consumidores em todo o mundo usando seus telefones celulares para verificar seus saldos de conta pelo menos uma vez nos últimos seis meses[2]. Os serviços bancários digitais parecem destinados a ficar, com 42% dos consumidores afirmando que não somente já utilizaram seus aplicativos para pagar suas contas, como também planejam continuar a fazê-lo no futuro[3].

Apesar da reação positiva dos consumidores e de seu crescente interesse em tecnologia, as instituições financeiras têm tido dificuldade em posicionar a tecnologia do banco digital como seu principal meio de engajamento do cliente. Isso se deve em grande parte aos muitos desafios que elas enfrentam atualmentenos procedimentos de onboarding e autenticação de dispositivos móveis.

Onboarding e Autenticação de Usuários do Aplicativos Financeiros Tradicionais

Os dois principais processos envolvendo qualquer cliente bancário ou de conta financeira são o cadastramento (ou onboarding) e o processamento da transação. Onboarding é o processo pelo qual os indivíduos iniciam sua jornada como cliente e, normalmente, é o ponto em que eles abrem uma nova conta. As transações, subsequentemente, normalmente constituem qualquer momento em que um cliente precisa acessar sua conta pessoal para movimentar dinheiro ou fazer alterações.

Historicamente, tanto o onboarding quanto o acesso à conta eram processos presenciais, exigindo que o titular da conta visitasse uma agência local. O funcionário na agência verificava a identidade da pessoa e atendia as necessidades especificadas do cliente. Com o uso da internet e dos smartphones, essa necessidade de um atendimento presencial começou a migrar para soluções digitais que podiam ser realizadas à distância. Hoje, a maioria das instituições financeiras oferece a seus clientes um meio de realizar transações online ou através de um aplicativo.

O processo de cadastramento, no entanto, ainda é geralmente um procedimento presencial. Isso se deve principalmente ao fato de que o onboarding é, em grande parte, um processo de verificação de identidade. Para as instituições financeiras em particular, conhecer seu cliente é fundamental para garantir que seus valiosos ativos e que os procedimentos subsequentes de acesso à conta estejam seguros e protegidos. Infelizmente, essa exigência presencial é cada vez mais inconveniente para os clientes.

Exemplos de Fraude

Os bancos estão familiarizados com as inúmeras maneiras com as quais os fraudadores persistem tentando corromper os seus sistemas; entre eles estão os "ataques de burla" que tentam enganar os mecanismos de segurança biométrica. Em casos mais comuns, a fraude é perpetrada não por estranhos, mas por familiares dos clientes ou mesmo funcionários da instituição financeira. Em ambos os casos, a biometria torna o onboarding e a autenticação mais resistentes a fraudes; porém, detecção de vida é necessária para prevenir que o fraudador se passe por suas vítimas. A seguir apresentamos alguns exemplos de ataques de burla e a prevenção oferecida pela função da detecção de vida.

Fraudes Internas

Uma categoria comum de fraude é cometida por uma pessoa conhecida e geralmente próxima; um membro da família, amigo ou colega de trabalho com acesso relativamente fácil aos dados de identificação de seu alvo. Esses dados são utilizados para se passar pela vítima ao abrir uma nova conta em seu nome ou para acessar uma conta existente sem seu consentimento. Usar o reconhecimento facial torna esses tipos de ataque muito mais difíceis; adicionando biometria de voz, ainda mais. Em ambos os casos, a detecção de vida é necessária para evitar que o criminoso use uma foto ou vídeo de sua vítima – um "ataque" – na tentativa de se passar por ela.

Uma categoria menos comum de fraude interna é perpetrada por funcionários do banco ou instituição financeira. Nesse caso, um funcionário coleta dados de identidade de um solicitante como parte de seu processo de onboarding, mas também tira uma foto ou faz um vídeo desse solicitante usando umdispositivo móvel . O requerente não percebe que isso não faz parte do processo padrão. O funcionário então usa as informações da conta e a imagem facial do cliente para criar e acessar essa nova conta; a linha de crédito do cliente acaba antes mesmo de ele começar a usá-la. A detecção de vida evita esse tipo de ataque interno.

Identidades Sintéticas

Outra categoria de fraude envolve a criação de "identidades sintéticas" que são criadas e usadas por fraudadores para obter crédito e empréstimos que eles nunca planejam pagar. Eles podem fazer isso repetidamente usando conjuntos de informações de identidade que são completamente fictícios ou baseados parcialmente em informações reais. A biometria facial pode ser usada para ajudar a proteger um processo de onboarding móvel contra o uso de identidades sintéticas. Mas sem a detecção de vida, um fraudador pode usar uma foto ou um vídeo de outra pessoa, ou ainda uma selfie com o rosto parcialmente obscurecido, o que evitaria que a imagem pudesse ser usada para vários mecanismos de validação biométrica. Mas sem a detecção de vida, um fraudador pode usar uma foto ou vídeo de outra pessoa, ou uma selfie com o rosto parcialmente obscurecido. Isso evita que a imagem seja usada para vários mecanismos de validação biométrica.

Os desafios atuais com o Onboarding

Embora o onboarding presencial seja um método testado e comprovado para cadastramento seguro de clientes, há uma série de desafios aos procedimentos atuais com os quais as instituições financeiras tem de lidar. O primeiro é a inconveniência. Com quase metade da população do planeta mais e mais acostumada a conduzir seus negócios através de seus smartphones, exigir que os clientes visitem uma agência é uma idéia cada vez mais desatualizada. Os clientes criaram expectativas de efetuar suas transações financeiras, como pagar suas contas e digitalizar cheques , através de seus smartphones. Portanto, ter que visitar uma agência para abrir uma conta passa a ter uma conotação negativa. A COVID-19 apenas exacerbou esse problema, incentivando as pessoas a confiarem em dispositivos móveis como jamais visto.

A experiência também mostra que os clientes vêem o processo presencial para abertura de conta como excessivamente demorado. Além do tempo de traslado, ter que esperar por um funcionário, processar a papelada e verificar os documentos de identificação é um processo longo do ponto de vista dos clientes. Aproximadamente 63% dos consumidores abandonaram um aplicativo devido ao tempo que o processo levou[4], representando um problema potencialmente bastante importante para as instituições financeiras.

Outro grande desafio para os procedimentos de onboarding atuais é como isso limita a capacidade de uma instituição em atrair novos clientes. As populações rurais representam uma grande oportunidade para os bancos, mas esses clientes nem sempre têm acesso à uma agência ou escritório local. Essa falta de acesso limita a capacidade dos bancos ou empresas de serviços financeiros de atrair novos clientes. Fornecer um processo de onboarding digital e seguro não só seria mais conveniente para os clientes existentes, mas também ajudaria a atrair novos clientes.

Por último, o onboarding digital introduz requisitos de compliance e risco de fraude. Por exemplo, um fraudador pode usar uma identidade roubada para abrir uma conta falsa em nome da vítima. O processo introduz risco associado a devida diligência em relação as informações do cliente e também a necessidade de conformidade regulatória. Este processo é frequentemente referido como "conheça seu cliente", ou KYC ("Know Your Customer"), e pode inibir a capacidade de um banco de oferecer serviços bancários digitalmente.

Os Desafios da Autenticação

Quando se trata de aplicativos de banco digital, a maioria usa senhas para autenticar usuários e conceder acesso a suas contas. Infelizmente, as senhas não são mais um método de autenticação segura, como evidenciado pelos relatórios quase diários com novos casos de violações de dados em grande escala ou fraude generalizada. Em 2017, descobriu-se que 81% de todas as violações de dados foram resultado de senhas inadequadas ou roubadas[5]. Essas senhas são frequentemente baseadas no que as pessoas conhecem, e os hackers podem roubar esse conhecimento por meio de phishing, ataques "man-in-the-middle" ou outros meios.

Além disso, os requisitos de senha se tornaram extraordinariamente complexos. Os consumidores precisam se lembrar de frases longas que consistem em caracteres alfanuméricos e não alfanuméricos. Além disso, a pessoa possui em média 92 contas registradas em um endereço de e-mail[6]. Para lembrá-las, as pessoas tendem a basear suas senhas em informações a que outras pessoas podem ter acesso facilmente e a usá-las em múltiplas contas. Portanto, embora as senhas estejam ficando mais complicadas, elas não são necessariamente mais seguras.

O custo dos ataques cibernéticos atingiu o setor bancário com força nos últimos anos, atingindo um custo médio de US $ 18,3 milhões anuais por empresa[7]. Atualmente, estima-se que mais de 70% de todas as violações de dados são motivadas financeiramente[8], colocando uma pressão crescente sobre os bancos e empresas financeiras para que tomem medidas para evitar que esses tipos de ataques sejam bem-sucedidos. O fato é que senhas não são mais seguras o suficiente para proteger nossos ativos financeiros e informações pessoais. Tanto para combater essas ameaças quanto para enfrentar os desafios atuais do onboarding, a biometria é uma solução ideal.

Os Benefícios da biometria no Onboarding e Autenticação de Usuários de Aplicativos Financeiros

Há uma série de razões pelas quais a biometria deve ser considerada como fator importante para bancos e instituições financeiras que buscam melhorar seus processos de onboarding e proteger seus ativos:

Dispositivos móveis:

o reconhecimento facial e de voz está emergindo como uma ferramenta útil para o onboarding de novos clientes e processos de "conheça seu cliente" (KYC). A biometria moderna está cada vez mais móvel, permitindo que novos clientes se cadastrem em serviços bancários por meio de seus smartphones e evitem uma visita à agência, o que é particularmente conveniente em áreas periféricas e rurais.

As soluções biométricas de hoje usam câmeras e microfones já presentes nos smartphones e dispositivos móveis atuais para realizar reconhecimento facial e de voz. Documentos de identificação, como carteiras de motorista ou passaportes, também podem ser associados a um indivíduo e verificados por meio do uso de "selfies" e funcionalidades biométricas. Ao colocar essas funcionalidades nas mãos do consumidor, os mesmos podem ser cadastrados em um sistema e posteriormente autenticados de praticamente qualquer lugar, aumentando a capacidade da empresa de atender de forma conveniente seus clientes atuais e de atrair novos clientes que atualmente estão indispostos ou impossibilitados de visitar uma agência.

No geral, esse processo biométrico móvel está provando ser tão eficaz quanto o realizado presencialmente por um funcionário do banco. É uma maneira conveniente e segura de os clientes confirmarem suas identidades sem visitar agências. E as imagens faciais ou amostras de voz podem ser usadas para funções de segurança no futuro.

Maior segurança:

com senhas cada vez mais se mostrando um método de autenticação pouco confiável e ultrapassado, a biometria serve como uma alternativa ideal para quem busca aumentar a segurança. O reconhecimento facial e de voz melhora a segurança de login ao exigir que o cliente forneça sua selfie e/ou amostra de voz. A biometria ao vivo é então comparada à informação biométrica armazenada durante o cadastramento e o acesso é concedido mediante uma autenticação positiva.

Uma vantagem importante é que, ao contrário das senhas, a biometria não pode ser roubada ou "adivinhada". A biometria usa algo que é único para cada pessoa - um rosto ou a voz - tornando muito mais difícil para os possíveis fraudadores a burlarem. A biometria também costuma apresentar algoritmos que realizam detecção de vida para determinar se um usuário é uma pessoa viva e presente, e não uma representação ou ataque de "spoofing" usando uma foto, vídeo ou máscara.

Com essas medidas biométricas em vigor, bancos e empresas financeiras podem ter certeza de que os clientes cadastrados não são impostores procurando abrir uma conta de forma fraudulenta e que seus procedimentos de autenticação não são mais suscetíveis a senhas propensas a fraude.

Maior conveniência:

a abertura de contas e autenticação são áreas em que a biometria melhora a segurança e a conveniência do mobile banking. Em contraste com a necessidade de lembrar uma senha de 12 caracteres e receber códigos de verificação por telefone, os clientes podem simplesmente tirar uma selfie quando precisarem acessar suas contas digitais.

A inclusão da biometria adiciona um nível de conveniência a quase todas as interações com o cliente. Por serem digitais, os clientes não precisam mais se deslocar até uma agência para abrir uma conta ou processar uma transação. A biometria móvel também é rápida, realizando uma autenticação de rosto e voz com detecção de vida em segundos. O processo é simples para os usuários, não exigindo etapas adicionais além de uma selfie ou gravação de uma amostra de voz. Por último, as soluções biométricas disponibilizam configurações flexíveis, colocando toda essa funcionalidade tanto no dispositivo móvel como no servidor, a fim de atender a particularidades dos recursos de rede disponíveis, e fornecer aos clientes uma solução biométrica em praticamente qualquer lugar do mundo.

Os clentes também expressaram interesse em usar a biometria para fins de autenticação. Aproximadamente 80% dos clientes acreditam que a verificação biométrica é mais segura do que métodos que envolvam nomes de usuário e senhas[9]. Quase 50% dos millennials já usam algum tipo de informação biométrica para autenticação própria. Além disso, 73% dos millennials e 68% dos indivíduos da Geração X acreditam que o reconhecimento facial é uma maneira fácil de identificação. Mesmo a maioria dos baby boomers acredita que o reconhecimento facial é uma opção de cadastramento e autenticação simples.

AWARE

Implementando Onboarding e Autenticação Seguros e Convenientes com Knomi

O Knomi® é uma plataforma de autenticação biométrica digital e uma poderosa opção para qualquer banco ou empresa de serviços financeiros que busque melhorar suas práticas de onboarding e/ou autenticação e se adequar aos desafios de hoje. O Knomi usa dispositivos presentes em qualquer smartphone para fornecer reconhecimento facial e de voz de maneira segura e conveniente para autenticação multi-fator digital.

Onboarding Digital:

o Knomi fornece prova de identidade para viabilizar o onboarding digital. Funcionalidades avançadas de segurança podem autenticar carteiras de motorista e passaportes, e garantir uma autenticação facial biométrica à prova de falsificações entre imagens vivas e impressas. O onboarding do Knomi inclui autenticação facial biométrica com documentos de identificação e verificação de mais de 9.000 documentos em todo o mundo. A detecção de vida do Knomi também detecta impostores, evitando que os mesmos abram contas de forma fraudulenta.

Autenticação Digital:

o Knomi fornece autenticação multifator sem senha usando reconhecimento biométrico facial e de voz e detecção de vida, e é baseado em algoritmos de correspondência de voz e rosto testados pelo NIST. Com os recursos biométricos multimodais do Knomi, os usuários podem ser autenticados com seus rostos, vozes, ou uma combinação dos dois para uma segurança ainda maior. O Knomi também pode ser configurado para muitos casos de uso diferentes, fornecendo a bancos e instituições financeiras os meios para personalizar a experiência do cliente para qualquer necessidade.

Detecção de Vida:

os algoritmos avançados de detecção de vida do Knomi detectam não apenas a falsificação da identidade da vítima, mas também a ocultação da identidade dos fraudadores, proporcionando aos bancos e empresas financeiras a tranquilidade de saber que seus clientes são quem dizem ser. A detecção de vida do Knomi também é simples para os usuários, não exigindo etapas adicionais (como movimentos de cabeça específicos) para ser eficaz. A solucão de prova de vida do Knomi funciona para processos de onboarding, autenticação e verificação de documentos.

Configurações Flexíveis:

além de funcionar com uma gama completa de sistemas operacionais, móveis e baseados em servidor, a plataforma Knomi está disponível em configurações centradas no dispositivo, no servidor, ou em navegadores. As configurações baseadas no dispositivo viabilizam a funcionalidade biométrica no dispositivo de uma pessoa e são ideais para situações em que a disponibilidade de rede não é garantida. As configurações baseadas no servidor, no entanto, colocam a funcionalidade biométrica no servidor; uma solução perfeita para quando há disponibilidade da rede. As configurações baseadas em navegador servem como uma terceira opção, realizando captura biométrica diretamente por meio de um navegador e incorporando funcionalidade adicional ao servidor. Seja qual for a escolha, Knomi fornece o mesmo nível de segurança e conveniência.

Como os bancos brasileiros e latino-americanos usam o Knomi para implementar onboarding digital.

Novos clientes são uma fonte indispensável para o crescimento da receita de qualquer banco, portanto cadastrá-los com eficiência está entre as funções mais importantes a se realizar. Mas o cadastramento também é um momento em que os bancos estão mais vulneráveis a fraudes. O cadastro é em grande parte um exercício de verificação de identidade, em que o banco tenta avaliar se um potencial titular de conta é confiável e pode receber uma linha de crédito, por exemplo.

Os bancos que incorporaram o software Knomi em seu processo de cadastramento podem utilizar a selfie ao vivo de um candidato a cliente para realizar várias verificações que servem para validar sua identidade e detectar quando há tentativa de fraude.

Diferentes versões do Knomi permitem que o processo seja conduzido a partir do aplicativo do banco ou, alternativamente, por meio de uma página da web em um dispositivo móvel ou desktop. Uma URL pode ser encontrada pelo requerente no site do banco, em um e-mail de propaganda ou em um anúncio em banner. Um cliente potencial simplesmente clica no link em seu celular ou desktop para iniciar o processo de abertura de conta em um navegador, o qual incluirá a captura de uma selfie ao vivo. Desta forma, um processo baseado em um navegador, aprimorado pela biometria, aumenta a segurança e reduz atritos comuns a um processo de cadastramento, sem exigir que o candidato instale um aplicativo antes de se cadastrar.

Os bancos brasileiros e latino-americanos estão usando o reconhecimento facial e a detecção de vida do Knomi para realizar uma variedade de verificações de identidade e detecção de fraude durante o cadastramento. A detecção de vida serve a alguns propósitos importantíssimos:

• Detecção de tentativas de personificação de uma vítima alvo usando "spoofs", como papel ou fotos 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 a detecção futura baseada no reconhecimento facial; e

• Não repúdio, que é um termo para descrever a capacidade de um banco de coletar evidências admissíveis em tribunal que associem a atividade de um fraudador a uma pessoa real; ou seja, evitar que o fraudador repudie seu envolvimento em uma tentativa de fraude.

Mas a detecção de vida também é uma parte essencial dessas outras medidas de segurança que dependem de autenticação e pesquisa biométrica, que estão sendo utilizadas por um ou mais clientes da Aware na região como parte de seus processos de cadastramento:

• **Match-to-ID da imagem facial.** Essa função, junto com a detecção de vida garante que o documento de identidade emitido pelo governo e usado para fornecer os dados de identidade seja autêntico e pertença ao requerente.

• **Análise de Duplicidades.** Imagens faciais de outros clientes são pesquisadas para garantir que o requerente não esteja tentando manter várias contas clandestinamente, usar uma identidade sintética ou assumir a identidade de um correntista existente.

• **Verificações de Lista Negra.** Bancos de dados de imagens faciais de fraudadores conhecidos são pesquisados para garantir que o requerente não seja um fraudador conhecido.

• **Verificações em agências externas (prestadores de serviço ou governo).** As imagens faciais podem ser submetidas a agências externas de segurança para determinar se os indivíduos têm antecedentes criminais.

Um exemplo de processo KYC móvel

1. Um consumidor faz o download do aplicativo de um banco e seleciona uma opção para se cadastrar como um novo cliente.
2. O aplicativo solicita que o consumidor mostre uma ou mais formas de identificação com foto.
3. Depois de registrar os documentos de identidade, o aplicativo obtém uma imagem ao vivo do rosto do cliente ("selfie").
4. O software de reconhecimento facial autentica (compara) a imagem ao vivo do cliente com o documento de identidade com foto.
5. A tecnologia também pode ser aplicada para verificar a autenticidade da identidade.

O futuro do banco digital está na biometria

As expectativas dos consumidores em relação a seus aplicativos de banco digital continuam a aumentar, principalmente ao deixarmos de usar o dinheiro em espécie. Eles esperam poder acessar suas contas e realizar transações virtualmente em qualquer lugar, sem comprometer a segurança. Por serem inerentemente mais seguras, convenientes e flexíveis do que as alternativas atuais, as soluções biométricas de hoje fornecem às empresas financeiras uma possibilidade de verificação de identidade poderosa e elegante para atender às necessidades e expectativas dos clientes de hoje.

Com a redução de viagens decorrente da COVID-19 e as taxas crescentes de roubo de identidade e violações de dados em todo o mundo, agora é o momento ideal para bancos e instituições financeiras considerarem enfrentar esses desafios incorporando a tecnologia biométrica aos seus procedimentos de cadastro e autenticação. Ao proteger seus clientes existentes, assim como atrair novos clientes, os bancos e outras instituições financeiras estão cada vez mais entendendo a biometria não apenas como uma necessidade aos negócios, mas como uma realidade.

Para obter mais informações sobre a plataforma de autenticação biométrica digital Knomi, entre em contato conosco ou visite nossa página na web.

Interessado em aprender mais sobre o Knomi? Visit www.aware.com/knomi/

Referências:

1 - www.bankmycell.com/blog/how-many-phones-are-in-the-world
2 - www.nielsen.com/us/en/insights/news/2016/digital-deposits-mobile-banking-around-the-world.html
3 - www.nielsen.com/us/en/insights/news/2016/digital-deposits-mobile-banking-around-the-world.html
4 - www.signicat.com/battle-to-onboard
5 - www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/ 6
6 - blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
7 - www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
8 - www.verizon.com/business/resources/reports/dbir/
9 - www.gigya.com/survey-reveals-52-percent-of-consumers-want-biometrics/