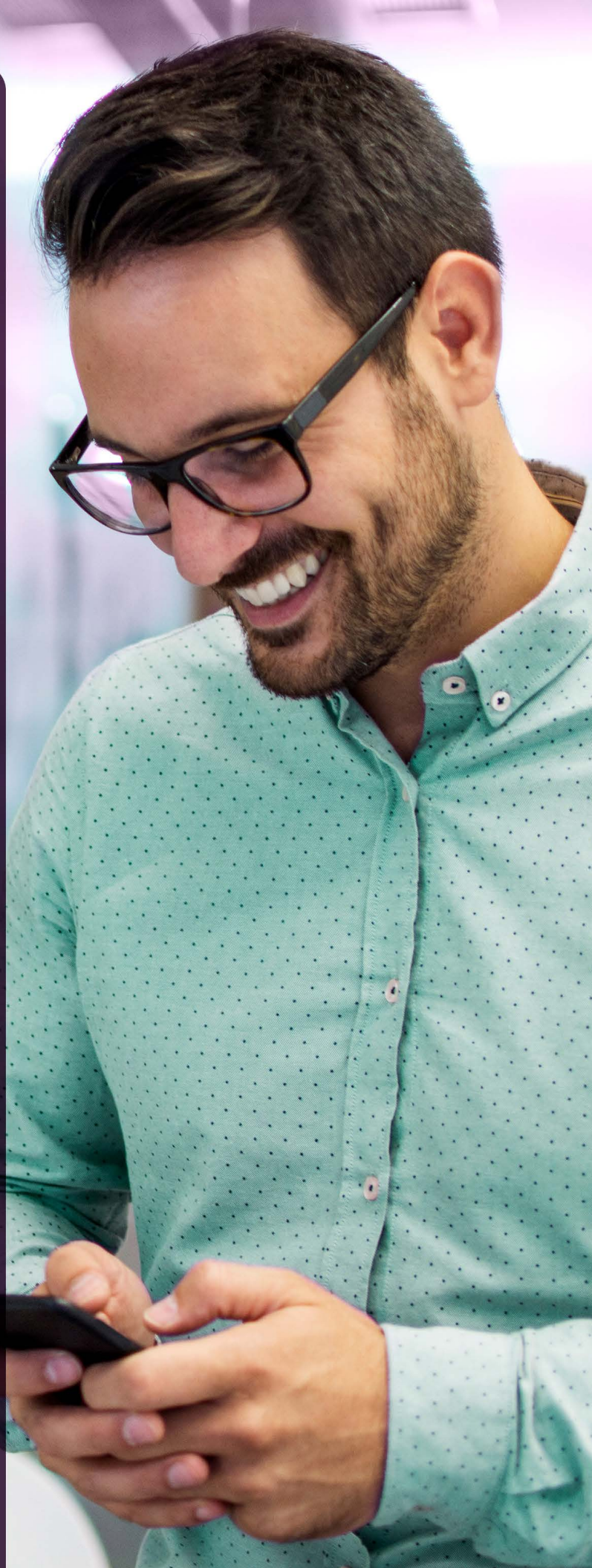
O guia definitivo para serviços financeiros

Como reduzir a fricção na autenticação prevenindo fraudes para usuários mobile



INCOGNIA™

Sumário executivo

Os negócios no mercado hoje em dia são cada vez mais mobile e as empresas do setor financeiro de todos os tipos precisam fornecer seus serviços para o usuário mobile de forma rápida e eficiente para se manterem competitivas. Estes serviços precisam ter menos fricção para os clientes, ao mesmo tempo em que os protege contra fraudes, incluindo o roubo de contas e fraude de identidade sintética, ambas em ascensão. Com os aplicativos para smartphones respondendo agora pela maior parte do tempo que as pessoas passam online[1], previsivelmente, as fraudes acontecendo via apps mobile estão aumentando à medida que os criminosos digitais, como dizem os americanos “follow the money”, ou vão aonde o dinheiro está.

Este whitepaper fornece uma análise e reflexão sobre o combate à fraude mobile, sem perder de vista a experiência sem fricções dos usuários. Incluímos uma visão geral das técnicas que os criminosos cibernéticos desenvolveram para explorar e superar a verificação de identidade e a autenticação multi-fator impostas pelas instituições. Também são fornecidas recomendações para uma nova abordagem tecnológica para combater esses ataques que tiram proveito das características inerentes à localização de dispositivos mobile. No mundo de hoje, nunca estamos sem nossos telefones celulares.

Nós os levamos para todos os lugares. Como resultado, nossos movimentos com estes dispositivos, sempre conectados, criam um padrão digital único ou o que chamamos de “fingerprint de localização”. A biometria comportamental por localização - ou seja, a representação anônima dos padrões de movimento de uma pessoa - acaba sendo inestimável para prevenir fraudes e fornecer serviços rápidos e sem fricção para usuários mobile - ambos objetivos de alta prioridade para as empresas de serviços financeiros nos dias de hoje.

1 Comscore, *Global State of Mobile* (2019)

O crescimento dos negócios significa o crescimento das contas mobile

Os negócios hoje em dia são cada vez mais mobile. Enquanto algumas empresas ainda dependem do tráfego de pedestres para uma parte relevante de sua receita, centenas de milhões de consumidores preferem usar canais mobile por sua simplicidade e conveniência.

Hoje, mais de 98% dos brasileiros acessam a internet pelo celular, inclusive na área rural onde 97% usam dispositivos mobile para estarem conectados. Ao passo que o celular é dominante, o uso de computadores perde força, caindo de 56% dos brasileiros na internet para 50%.[2] Estima-se que até 2025, 72% de todos os usuários de internet no mundo inteiro só acessarão a internet através de smartphones[3].

Até 2025, 72% de todos os usuários de internet só terão acesso à internet através de smartphones.

Atualmente, cerca de 2,4 bilhões de pessoas usam smartphones para serviços financeiros, e o uso de smartphones para compras e gerenciamento financeiro só aumentou durante a pandemia da COVID-19. Agora, cerca de um terço dos clientes de bancos espera usar mais os serviços bancários mobile e online mesmo quando a pandemia acabar[4].

Mesmo que um cliente abra uma conta em uma agência bancária, é provável que ele acesse sua conta em um dispositivo móvel. Isto é especialmente verdade para a Geração X e Millennials - a grande maioria dos quais possui smartphones[5].

A popularidade dos telefones celulares tem implicações importantes para as empresas de serviços financeiros:

Os canais mobile são essenciais para o sucesso

As empresas devem ser capazes de dar suporte aos clientes que abrem conta e transacionam em dispositivos mobile.

Os canais mobile devem ser seguros

As empresas devem ser capazes de enfrentar as vulnerabilidades de fraude inerentes aos serviços financeiros online em geral, e em dispositivos mobile especificamente.

As experiências mobile devem ser impecáveis

Quaisquer que sejam os serviços fornecidos via smartphones, devem atender às expectativas dos usuários mobile de experiências rápidas e sem fricções.

A coleta de dados deve estar em conformidade com as leis de privacidade

Qualquer coleta e armazenamento de dados em um app mobile deve seguir as normas de privacidade de dados, como no Brasil, a LGPD.

Os canais mobile devem estar em compliance com as regulações

As normas e regulações do sistema financeiro precisam ser seguidas, como boas práticas de antifraude.

2 Agência Brasil, *Celular é o principal meio de acesso à internet no país,* (Abril de 2020)

3 CNBC, *Nearly three quarters of the world will use just their smartphones to access the internet by 2025,* (Janeiro de 2019)

4 The Financial Brand, *Big Banks Benefiting Most from COVID-19 Digital Shifts,* (2020)

5 Pew Research Center, *Millennials stand out for the technology use, but older generations also embrace digital life,* (Setembro de 2019)

Desafios da verificação e autenticação de identidade mobile

A verificação de identidade e a autenticação contínua são requisitos fundamentais para qualquer aplicativo mobile de serviços financeiros. As empresas precisam estar confiantes de que sabem quem está abrindo uma conta, quem está entrando nessa conta e quem está executando transações associadas a essa conta.

Mas a verificação e autenticação de identidade em um telefone celular apresentam desafios únicos para equilibrar fraude e fricção.

- **Prevenção de fraudes**
  As empresas de serviços financeiros precisam validar os novos usuários e autenticar os clientes que voltam às plataformas mobile sempre que acessam sua conta ou realizam uma transação de alto risco, como uma transferência de valores.

- **Experiência sem fricção**
  Toda interação mobile com os clientes precisa ser rápida, com o mínimo de telas possível e sem fricção, para que os clientes não fiquem frustrados e usem outro site ou app, a um clique de distância.

- **Privacidade**
  É essencial que todo aplicativo mobile que coleta, opera e armazena dados de usuários respeite a privacidade do cliente, conforme exigido pela Lei Geral de Proteção de Dados, a recém aprovada LGPD.

- **Conformidade regulatória**
  Qualquer procedimento de identificação de usuários precisa estar em conformidade com uma série de normas do Conselho Monetário Nacional e Banco Central sobre checagem, contínua, de autenticidade dos dados (Resolução 4.753/19)[6], boas práticas de segurança nos serviços financeiros, o que resulta na necessidade de medidas antifraude (Resolução n° 3.694/09)[7], e procedimentos de Know Your Customer (KYC) (Resolução n°3.978/20[8] e Lei 9.613/98 - Lei de Prevenção à Lavagem de Dinheiro)[9].

Destes três desafios, a prevenção da fraude é a mais complicada. Os criminosos cibernéticos têm mais ferramentas, técnicas e dados roubados para trabalhar do que nunca, e isso se reflete em dados: A fraude financeira aumentou 104% apenas no primeiro trimestre de 2020.[10]

A fraude financeira aumentou 104%
apenas no primeiro trimestre de 2020.

6 Resolução *4.753/19 do Bacen* (Setembro de 2019)

7 Resolução *3.694/09 do Bacen* (Março de 2009)

8 Resolução *3.978/20 do Bacen* (Janeiro de 2020)

9 Lei N° 9.613 *Dos Crimes de "Lavagem" ou Ocultação de Bens, Direitos e Valores* (Março de 1998)

10 *Security Boulevard, Financial fraud reports in the US jumped by 104% in 2020 Q1* (Junho de 2020)

As empresas devem ter a expectativa de que a fraude continue sendo um desafio importante nos próximos anos.

Embora a prevenção de fraudes possa ser o mais difícil destes desafios, todos os três são importantes e inter-relacionados. De fato, abordar a fraude de forma a aumentar a fricção para o cliente é uma proposta negativa para as empresas. Embora a meta seja reduzir as perdas por fraudes, quando os controles de segurança frustram os clientes, o resultado é uma queda no consumo, conversões menores e, em última instância, efeitos negativos sobre a receita financeira.

Desafio #1:
Previnir a fraude em dispositivos mobile

Os cibercriminosos vão aonde está o dinheiro. Eles utilizam a automação e os dados para executar seus crimes. Vejamos o jogo de gato e rato que empresas de serviços financeiros e criminosos jogam regularmente com a segurança de contas em dispositivos mobile, concentrando-se especificamente em dois vetores de ataque mais comuns:

Fraude de identidade sintética
Em que os criminosos combinam informações pessoais de pessoas reais com dados falsos para criar uma identidade produzida para a abertura de contas fraudulentas.

Ataques de roubo de conta
Em que os criminosos ganham acesso à conta de um cliente legítimo e a utilizam para roubar fundos ou cometer outros crimes financeiros.

Fraude de identidade sintética

Com todas as informações pessoais e privadas prontamente disponíveis aos fraudadores, não é surpresa que o roubo de identidade esteja em ascensão. Em 2019, os consumidores relataram 3,2 milhões de casos de roubo de identidade à Comissão Federal de Comércio (FTC) nos Estados Unidos. Desses, 1,7 milhões de denúncias envolveram fraude, e em 23% desses casos, os consumidores perderam dinheiro - um total de US$ 1,9 bilhões cumulativamente,

3,2 milhões de casos de roubo de identidade foram relatados em 2019.

representando um aumento de US$ 238 milhões em relação a 2018[11]. Desde o início da pandemia da COVID, as taxas de roubo de identidade e de fraude ao consumidor aumentaram ainda mais acentuadamente, à medida que os fraudadores se aproveitam de informações públicas para se fazer passar por consumidores qualificados para o seguro-desemprego, ou outras formas de auxílio governamental.

A fraude de identidade sintética é a forma de crime financeiro que mais cresce nos Estados Unidos, custando US$ 6 bilhões anualmente de acordo com o Federal Reserve[12]. Este tipo de fraude ocorre quando os fraudadores combinam dados de identidade legítimos e falsos para criar uma identidade falsa e "sintética". Podem ser usados o nome e o número do CPF legítimos de uma pessoa, o endereço de outra, e o número de telefone de outra. Os fraudadores usam esses elementos para criar uma pessoa fictícia e depois abrem novas contas em bancos e outras empresas on-line. Eles realizarão negócios legítimos com essas contas durante meses ou mesmo anos, construindo um histórico idôneo com a identidade sintética com o propósito de eventualmente executar uma transação com um alto pagamento. A recompensa típica por incidente nos Estados Unidos é de $10.000 a $15.000.

A fraude com identidade sintética é a forma de crime financeiro que cresce mais rapidamente

Infelizmente, este é um tipo de fraude que é notoriamente difícil de ser detectada. De acordo com o Fed, os modelos de detecção de fraude comumente usados falham na identificação da fraude de identidade sintética em 85% a 95% dos casos[13]. Técnicas de prevenção de fraude destinadas a evitar o roubo de conta - técnicas como a autenticação multi-fator - são em grande parte impotentes para deter os fraudadores uma vez que eles tenham tentado e conseguido abrir uma conta com credenciais de trabalho.

Os modelos de detecção de fraude mais comuns não identificam a fraude de identidade sintética em 85% a 95% dos casos.

Essa forma de fraude é mais eficazmente combatida na abertura da conta, e isso é muito importante. Uploads de documentação inconvenientes e demorados para verificar a identidade dos usuários podem impactar negativamente o crescimento dos negócios.

11 Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime,* (2020)

12 CNBC, *Criminals are using 'Frankenstein identities' to steal from banks and credit unions,* (Janeiro de 2020)

13 Federal Reserve Banks, *Payments Fraud Insights: Detecting Synthetic Identity Fraud in the U.S. Payments System,* (Outubro de 2019)

Roubo de contas mobile

As empresas de serviços financeiros e outros negócios têm uma variedade de meios para se protegerem contra as fraudes de roubo de conta, mas a fraude ainda está aumentando. Os fraudadores continuam a encontrar formas de contornar as barreiras de segurança. Vamos dar uma olhada nessas técnicas de defesas e por que elas ainda não são o suficiente.

Autenticação multi-fator

Para se proteger contra a fraqueza inerente dos nomes de usuário e senhas, muitas empresas recorrem à autenticação multi-fator (MFA), exigindo que os clientes complementem sua senha com alguma outra informação ou interação para verificar sua identidade. Este fator de autenticação pode ser:

- Uma senha de uso único (OTP)
  Um número único, gerado aleatoriamente, enviado por SMS ou notificação push para o telefone celular do titular da conta, para que o cliente possa inseri-lo em um formulário on-line, demonstrando a propriedade (ou pelo menos o controle) de um dispositivo mobile previamente autenticado.
- Um código único de um aplicativo autenticador
  Um código numérico de um aplicativo mobile que gera automaticamente um número aleatório reconhecido por um website ou outro aplicativo mobile.
- Autenticação baseada em conhecimento (KBA)
  Uma pergunta projetada para exigir que o cliente introduza informações não públicas que só ele saberia, verificando assim, ostensivamente, a identidade do cliente.

Pontos fracos da autenticação multi-fator (MFA)

Embora a MFA seja um passo importante para aumentar a segurança das contas de clientes e é definitivamente uma melhoria no uso de apenas um nome de usuário e senha, a realidade é que até mesmo o MFA está sendo burlado usando uma variedade de ataques.

Fraude de troca SIM ou Sim Swap

As mensagens SMS podem ser interceptadas de diversas maneiras, permitindo que os criminosos digitem códigos seguros destinados apenas a clientes legítimos. Talvez a maneira mais eficaz de interceptar mensagens SMS seja fazer uma troca de SIM.

Os criminosos virtuais descobriram como usar a engenharia social para transferir a propriedade da conta de um cartão SIM para outro. Por exemplo, um fraudador liga para uma empresa de telecomunicações se passando por um cliente legítimo que teve seu telefone perdido ou roubado e convence um agente de atendimento ao cliente a transferir o número de telefone do cliente para um cartão SIM de sua propriedade. Uma vez que a conta tenha sido transferida, chamadas telefônicas e mensagens SMS irão diretamente para o telefone celular do criminoso. O criminoso pode então usar seu telefone para interceptar as mensagens SMS usadas para verificar a identidade do cliente quando bloqueado fora de uma conta ou quando mudar as senhas. Muito rapidamente, o criminoso pode obter acesso a contas de e-mail, contas de mídia social, e-commerce e contas de serviços financeiros. Quando a fraude é descoberta, compras podem ter sido feitas e quantias financeiras já ter sido transferidas e perdidas.

Devido à crescente popularidade dos ataques de troca de SIM, os especialistas em segurança agora desencorajam o uso de SMS como forma de segundo fator de autenticação[14]. Mesmo quando as mensagens SMS não são interceptadas, às vezes chegam tarde ou não chegam, frustrando os clientes que estão tentando entrar em suas contas para concluir uma transação rápida e facilmente.

14 CNET, *Do you use SMS for two-factor authentication? Here's why you shouldn't,* (Abril de 2020)

Malware em apps de autenticação

Os aplicativos autenticadores são mais confiáveis e seguros do que as mensagens SMS. Alguns, porém, têm se mostrado suscetíveis a malware e muitos são vulneráveis a ataques contra sistemas operacionais antigos[15].

Engenharia social de autenticação baseada no conhecimento

As perguntas baseadas em conhecimento há muito tempo são consideradas problemáticas. As perguntas são freqüentemente sobre residência anterior, nome dos pais ou sobre os nomes de escolas, animais de estimação ou professores. Muitas vezes os clientes não se lembram das respostas corretas; outros 10-15% das vezes, não reconhecem nenhuma das escolhas que estão sendo fornecidas, e ficam frustrados por lhes ser perguntado algo que não são capazes de responder[16]. Mais preocupante é que, devido às mídias sociais e violações de dados, uma grande quantidade de informações aparentemente privadas são prontamente descobertas por criminosos dispostos a fazer uma pesquisas bem breve. Explorar o Facebook e o LinkedIn, por exemplo, muitas vezes revela os aniversários, assim como os nomes de parentes, animais de estimação, escolas, e domicílios, tornando esses tópicos inúteis para a prevenção de fraudes.

Claramente, basear a segurança da conta na suposta privacidade de tais dados prontamente disponíveis é um erro. Enquanto algumas empresas de serviços financeiros ainda confiam na autenticação baseada em conhecimento (KBA), outras estão eliminando gradualmente este tipo de autenticação e buscando técnicas mais confiáveis para verificação de identidade e prevenção de fraudes. Em última instância, qualquer forma de autenticação que se baseie em informações estáticas, tais como históricos de endereços, é suscetível a erro ou comprometimento pela engenharia social e provavelmente introduz fricção e frustração na experiência mobile dos clientes.

Biometria

A biometria, incluindo as impressões digitais e o reconhecimento facial, estão entre os fatores mais recentes a serem utilizados para a autenticação de multi-fator. Embora mais complicados que as senhas, e portanto mais difíceis de imitar ou forjar, infelizmente são igualmente vulneráveis a serem roubados. Qualquer forma de credencial estática é problemática como uma credencial de autenticação, pois uma vez roubada ela pode ser usada para roubar as contas. Isto é especialmente problemático para algumas tecnologias de biometria, pois os usuários não têm a opção de alterar suas características físicas, como fariam com uma senha.

Desafio #2:

Como entregar uma experiência mobile rápida e sem fricção

Os consumidores estão acostumados a interações rápidas em dispositivos mobile. Se eles podem fazer compras, verificar o clima, chamar um serviço de transporte privado e pedir uma refeição rápida e facilmente, eles esperam também poder conduzir transações financeiras rápida e facilmente.

15 Tom's Guide, *Don't run your 2FA authenticator app on these smartphones,* (Fevereiro de 2020)

16 Gartner, *When Knowledge-Based Authentication Fails, and What You Can Do About It,* (Setembro de 2012)

As empresas de serviços financeiros precisam respeitar o tempo do cliente mobile, porém as interações em apps são muitas vezes lentas e frustrantes. Isto é especialmente verdade em um momento crítico: a abertura de conta. Apenas 8% dos clientes de bancos conseguiram abrir contas usando um dispositivo mobile[17], com sucesso, na verdade, cerca de um em cada cinco clientes potenciais que solicitam contas financeiras em dispositivos mobile abandonam suas tentativas de abertura de conta antes de concluí-las[18]. Outro estudo concluiu que 40% dos consumidores abandonam o processo de onboarding em instituições financeiras, citando a quantidade de tempo necessária e a quantidade de informações pessoais solicitadas[19]. O tempo necessário para abrir uma conta está inversamente relacionado com a porcentagem de clientes que completam o processo de abertura de conta. Pesquisas mostram que adicionar apenas cinco minutos ao processo de abertura de conta pode aumentar as taxas de abandono em 200%[20].

Apenas 8% dos clientes de bancos puderam abrir contas com sucesso usando um dispositivo mobile.

A realidade é que experiências mobile lentas e incômodas estão custando às empresas de serviços financeiros clientes valiosos. Isso é especialmente verdade com Millennials, que são especialistas em tecnologia e interessados em produtos de serviços financeiros, como contas de poupança e investimentos, financiamentos imobiliários e outros tipos de empréstimos.

A adição de apenas cinco minutos ao processo de onboarding pode aumentar as taxas de abandono em 200%.

> **56.3%** de todos os Millennials abandonariam um processo de aquisição de um produto de serviços financeiros se não pudessem completá-lo em seu dispositivo mobile e, em vez disso, mudariam para um concorrente mais amigável[21].
>
> **42.4%** dos Millennials deixaram um prestador de serviços financeiros devido a uma má experiência mobile[22].

O resultado final: Quaisquer que sejam os métodos que as empresas de serviços financeiros escolham para combater o roubo de identidade sintética, roubos de contas e outros tipos de fraude, os usuários não são pacientes com a segurança que torna a abertura de contas e outras transações comerciais lentas, incômodas ou confusas. A experiência do usuário é um fator de "make-or-break" para empresas on-line, ou seja, as que não fornecerem uma experiência excelente, estarão fora do jogo, especialmente com consumidores "nativos digitais" Millennials e da Geração Z.

17 Javelin Research, *Digital Account Opening Still Has a Long Road to Reality,* (Fevereiro de 2017)

18 Forbes Why Can't Banks Get Digital Account Opening Right?, (Outubro de 2019)

19 American Banker, BankThink: Why Mobile Onboarding Is Such a Turnoff, (Julho de 2019)

20 Significat, Digital Banking Report (2016)

21 Mitek, *Research reveals millennial demographic "meaningless" for financial institutions and "Fin-techs"* (Novembro de 2016)

22 Ibid.

Desafio #3:

Conformidade com as normas de privacidade de dados

Ao mesmo tempo em que as empresas de serviços financeiros estão tentando combater a fraude, há a exigência adicional de garantir o cumprimento de uma ampla gama de regulamentos, que agora incluem regulamentos de privacidade de dados, como a LGPD, a GDPR e o CCPA. Os requisitos de privacidade variam de país para país e região para região, mas em geral, as regulamentações exigem:

Minimização de coleta de dados

Coleta apenas dos dados absolutamente necessários para os negócios que estão sendo conduzidos.

Segurança dos dados

Proteger os dados do consumidor contra violações e vazamentos e contra exposição desnecessária dentro da organização.

Revisão, correção e exclusão de dados

Permitir ao consumidor solicitar acesso aos seus dados para saber o que está sendo coletado, para que os erros possam ser corrigidos e, quando solicitado, para que os dados sejam apagados se essa eliminação não violar outras leis e regulamentos.

Atualmente, 66% dos países aprovaram regulamentações sobre privacidade de dados, e mais regulamentações estão sendo elaboradas e discutidas[23]. Estas leis estão sendo escritas e aprovadas em resposta às crescentes preocupações do público com a privacidade dos dados, violações e vazamentos de dados e exposição involuntária à fraude. Mais da metade dos adultos dos Estados Unidos deixaram de usar um produto ou serviço por causa de preocupações com privacidade[24]. Para ganhar a fidelidade de clientes como estes, as empresas devem levar a sério a privacidade dos dados. Especificamente no Brasil, com a LGPD prestes a entrar em vigor, os clientes, em tese, estarão mais protegidos e as empresas que estiverem bem preparadas, terão segurança jurídica como controladoras ou operadoras dos dados. Podemos esperar consumidores cada vez mais de olho nas práticas de privacidades das empresas.

As organizações de serviços financeiros devem esperar que a privacidade de dados cresça em importância nos próximos anos. Quaisquer que sejam as soluções de segurança implementadas para combater a fraude, também é necessário proteger a privacidade dos dados.

O Desafio #4:

Compliance com as normas de segurança e antifraude

Compliance com as normas de segurança e antifraude Conselho Monetário Nacional e o Banco Central do Brasil, que estabelecem o regramento da prestação de serviços financeiros, têm atualizado suas

23 United Nations Conference on Trade and Development, *Data Protection and Privacy Legislation Worldwide,* (Julho de 2020)

24 Pew Research Center, *Half of Americans have decided not to use a product or service because of privacy concerns,* (Abril de 2020)

normas para incluir novas tecnologias no sistema financeiro, ao mesmo tempo que garantem a segurança dos usuários e legalidade das transações. Os objetivos de muitas dessas normas são a autenticidade dos dados dos usuários, tornar os serviços mais dinâmicos e adaptados à realidade digital, segurança e a prevenção à lavagem de dinheiro e financiamento ao terrorismo (PLDFT).

Novas tecnologias para autenticação do usuário e práticas de segurança

A Resolução 4.753/19 veio para reforçar essa tendência. Deixou de exigir a apresentação de ficha-proposta pelo usuário e, em conjunto com a Circular nº 3.694, define que basta que haja documentação hábil a confirmar a autenticidade dos dados, sem limitar quais são os meios possíveis. Em acréscimo, autoriza que os dados fornecidos sejam autenticados através de base de dados, estimulando o uso de tecnologia no momento de validar o endereço e outras informações cadastrais de quem está criando uma conta digital.

Essa resolução permite o uso de ferramentas eletrônicas, como a geolocalização e a biometria, para a validação de dados de clientes e ainda indica que não basta usá-las no momento do onboarding, é preciso que a verificação da autenticidade e atualidade seja recorrente. Focando na validação de endereço, a nova resolução abre caminho para alavancagem do fechamentos de contratos entre instituições financeiras/de pagamento e clientes e para redução da taxa de abandono no onboarding na etapa de comprovação dos dados cadastrais.

O uso de tecnologias precisas e assertivas de autenticação dialoga diretamente também com os padrões de boas práticas bancárias, previstas na Resolução nº3.694/09, como o dever de buscar a integridade, a confiabilidade, a segurança e o sigilo das transações realizadas, bem como a legitimidade das operações contratadas e dos serviços prestados.

Procedimentos de Know your Customer (“KYC”)

Por força de Lei, as instituições financeiras e instituições de pagamentos, dentre outras entidades, estão obrigadas a adotar mecanismos para prevenção à lavagem de dinheiro e financiamento ao terrorismo, e isso leva a implantação de procedimentos de KYC, como previsto na Resolução nº3.978/20 do CMN. Dessa forma, as instituições sujeitas à essa regulação devem buscar conhecer, qualificar e classificar os clientes e prestadores de serviços (e os beneficiários finais, no caso das Pessoas Jurídicas) para identificar e mensurar o risco de utilização de seus produtos para fins ilícitos. Devem também implementar Política interna de PDLFT e estrutura de governança adequada, estabelecendo seus critérios e formas de avaliação de risco, além de outras obrigações.

Equilibre fraude, fricção e conformidade no mobile

Há algumas boas notícias para enfrentar os desafios do combate à fraude ao oferecer um serviço rápido e sem fricções para usuários mobile. Como os clientes carregam seus telefones com eles em todos os lugares, o registro de seu deslocamento proporciona um padrão de comportamento único ou fingerprint de localização que pode ser usado para verificar a identidade dos indivíduos tentando abrir conta e autenticar os clientes com onboarding já feito.

Esta abordagem tecnológica para a prevenção de fraudes é conhecida como biometria comportamental por localização e oferece o benefício de ser sem fricção para os usuários, mas rígida para os fraudadores.

A biometria comportamental por localização oferece o benefício de ser sem fricção para os usuários, mas rígida para os fraudadores.

Ao combinar sinais de uma variedade de tecnologias, incluindo GPS, Wi-Fi, Bluetooth e outros sensores no dispositivo, é possível identificar a localização de um telefone celular a menos de 3 metros - uma precisão muito maior do que aquela fornecida apenas por GPS ou localização por Wi-Fi.

Quando este comportamento de localização é continuamente anônimo, criptografado e hasheado, a privacidade do usuário é protegida e fornece uma nova camada inestimável de verificação de identidade e prevenção contra fraudes. Usando a biometria de comportamento por localização, as empresas de serviços financeiros podem adicionar um sinal de risco adicional indicando se o comportamento de localização atual de um usuário de telefone celular corresponde ou não ao fingerprint de localização de determinado cliente.

Biometria comportamental por localização a serviço de um usuário mobile

Aqui estão exemplos de como a biometria comportamental por localização ajuda a proteger as empresas de serviços financeiros e seus clientes:

Abertura de conta nova

Um novo cliente baixa o aplicativo mobile de um banco e solicita uma conta bancária, fornecendo seu endereço residencial no processo. Em segundo plano, o aplicativo faz uma solicitação para um serviço de biometria comportamental por localização que compara os dados de localização do smartphone com os dados de endereço fornecidos pelo solicitante. Se o solicitante listar um endereço de casa ou do trabalho que não se encaixa com os dados de seu comportamento usual de localização, o aplicativo receberá uma pontuação de alto risco indicando inconsistência. O banco pode então solicitar mais informações ao solicitante ou rejeitar a solicitação diretamente, dependendo de suas políticas.

Identificação multi-canal

Um novo solicitante solicita uma conta em uma fintech em seu computador desktop em casa, mas também tem o aplicativo mobile da fintech em seu telefone. O solicitante lista seu endereço residencial e número de telefone celular. A aplicação web contacta o serviço para verificar os dados de localização anônimos no telefone celular e compará-los com o endereço residencial fornecido. Se os dados de localização corresponderem ao endereço residencial indicado pelo solicitante, uma pontuação de baixo risco é devolvida, indicando que o usuário é provavelmente legítimo. O serviço da fintech procede com a abertura de conta.

Transações seguras

Um cliente bancário em um telefone celular tenta transferir a maior parte dos fundos da conta para uma conta em outro banco. O serviço determina que a localização do dispositivo utilizado para solicitar a transferência não corresponde ao histórico de localização do dispositivo anteriormente associado ao perfil do cliente, talvez porque a conta tenha sido comprometida. O serviço envia um alerta, para que o banco possa bloquear a transferência e a equipe de fraude do banco possa contatar o cliente para investigar a situação.

A solução de Incognia

Incognia é o líder do setor em utilizar a biometria comportamental por localização para oferecer uma solução de identidade privada e autenticação para reduzir a fricção para usuários legítimos ao mesmo tempo que previne fraudes mobile. A solução Incognia utiliza dados de localização anônimos e criptografados, capturados diretamente de sinais de rede e sensores no dispositivo, para construir um padrão de comportamento único que é usado para identificar e autenticar usuários mobile durante o onboarding, login e transações. O uso de dados comportamentais dinâmicos, não estáticos de identificação pessoal (PII), permite que a Incognia forneça às empresas de serviços financeiros uma camada extra de segurança que é adaptativa e privada, protegendo-as contra novas técnicas de fraude.

A solução Incognia oferece proteção contra fraudes em momentos críticos da jornada do usuário:

01

Onboarding
O serviço Incognia compara os dados de localização do smartphone com o endereço fornecido no onboarding. Se detectar uma localização anômala, o serviço Incognia retorna uma pontuação baixa ou nenhuma correspondência que alerta a instituição sobre o risco potencial.

02

Login
Para proteger do roubo as contas existentes, Incognia fornece uma camada de segurança silenciosa e em segundo plano para garantir que o dispositivo que entra em uma conta tenha um comportamento de localização que corresponda ao comportamento esperado do proprietário desta conta.

03

Transaction
Antes de realizar uma transação de alto risco, como uma retirada ou transferência de alto valor, um aplicativo mobile pode solicitar uma pontuação de risco de Incognia para garantir que a localização atual do smartphone corresponda ao comportamento histórico do dispositivo associado à conta.

Enquanto os exemplos acima representam os casos de uso mais comuns, a pontuação de risco de Incognia pode ser utilizada de acordo com as especificações do cliente. Casos de uso adicionais incluem a redefinição de senha, a inclusão de métodos de pagamento adicionais, ou a edição de informações de conta.

A solução Incognia oferece benefícios exclusivos para empresas de serviços financeiros e seus clientes mobile:

Adaptiva

- Utiliza dados comportamentais em tempo real para prova avançada de identidade e autenticação
- Cria uma identidade digital dinâmica que não pode ser prevista ou falsificada

Sem fricção

- Proporciona maior segurança sem fricção adicional
- - Funciona silenciosamente em segundo plano, não requerendo nenhuma ação do usuário

Privacy-first

- Utiliza tecnologia proprietária de anonimização de localização
- Não coleta ou armazena intencionalmente nenhuma outra forma de dado identificável, incluindo nomes, CPFs, números de telefone e endereços de e-mail

A integração de Incognia em aplicações mobile é rápida e fácil e normalmente leva menos de 30 minutos. Incognia fornece um Kit de Desenvolvimento de Software (SDK) e APIs totalmente documentados. Quando ativado em um aplicativo mobile, Incognia normalmente consome menos de 0,5% da vida útil da bateria em 24 horas.

Estudo de caso de banco mobile

Ao integrar Incognia em seu aplicativo mobile, um dos principais bancos de varejo do Brasil pôde verificar automaticamente 85% de todos os novos pedidos de abertura de conta mobile que recebeu.

38% Aumento em contas mobile abertas

63% Redução em falsos positivos (transações e aberturas de conta acusadas como fraude erroneamente)

24% Redução em revisão manual de risco, poupando tempo e dinheiro

10 Identidades falsas descobertas

Incognia ajuda as empresas de serviços financeiros a aumentar as contas, melhorar a experiência do cliente, combater a fraude e agilizar as operações de back-office.

Sumário

Neste whitepaper, examinamos as exigências dos usuários mobile para verificar identidades e prevenir fraudes, ao mesmo tempo em que as experiências precisa ser rápidas e sem fricção. Também examinamos os pontos fortes e fracos das tecnologias de segurança aplicadas ao usuário mobile, incluindo o uso de autenticação multi-fator (MFA), aplicativos autenticadores e interações com perguntas de conhecimento (KBA) para combater a fraude em dispositivos mobile. Finalmente, consideramos os benefícios que o comportamento anônimo de localização dos smartphones pode proporcionar para melhorar a velocidade e a precisão dos processos de verificação e autenticação de identidade dos usuários mobile.

Desenvolvido como resultado de quase uma década de experiência com tecnologia de localização mobile, Incognia oferece às empresas de serviços financeiros o serviço de verificação de identidade rápido e rigoroso que elas precisam para autenticar os clientes mobile e derrotar os fraudadores, sem acrescentar fricções para os usuários. Incognia é uma solução de segurança mobile construída para o mundo mobile.

Clique para saber mais sobre a solução Incognia →

Sobre a Inloco e Incognia

Inloco é uma empresa de identidade privada baseada na tecnologia de localização. Incognia é o produto que permite a prevenção de fraudes mobile para bancos, fintechs e e-commerces usando biometria comportamental baseada em localização, e oferece verificação e autenticação de identidade sem fricção. Temos sede em Recife e São Paulo, e nossa empresa-irmã que leva o mesmo nome do produto de prevenção à fraudes, Incognia, tem escritórios em Palo Alto e Nova Iorque. Temos atualmente mais de 60M+ de dispositivos com nossa tecnologia de localização.

Utilizamos dados comportamentais de localização para aumentar a segurança da conta de usuários, reduzir fraudes e fornecer serviços de localização privada sensíveis ao contexto. Nossa tecnologia utiliza sinais de rede e sensores no dispositivo para fornecer informações de localização altamente precisas. Ao construir um padrão de comportamento anônimo, único para cada usuário, Incognia fornece contexto de localização e cria uma identidade digital privada para a segurança das contas.

Empresas com aplicativos móveis e dispositivos conectados usam Incognia para verificação de identidade de usuários sem fricção, autenticação dinâmica adaptativa, avaliação de risco e detecção de fraude, tudo isso enquanto protegem a privacidade do usuário.

Privacidade

A privacidade do usuário é uma preocupação central da Inloco. A arquitetura de nossos produtos é feita sob os princípios do privacy by design, implementando técnicas de proteção da privacidade desde a concepção até o uso final de nossos produtos e soluções.

A tecnologia da Inloco foi projetada para impedir o acesso à informação capaz de re-identificar os usuários. Isto significa que a Inloco não coleta identificadores de dispositivos estáticos únicos (tais como IMEI e MAC), contas associadas (e-mail e telefone), dados de identificação civil (nome e CPF), bem como alguns dados sensíveis como informações que revelam etnia, religião, opinião política, religião, filosofias, entidades políticas ou sindicais ou dados sobre saúde, vida sexual, genética e biometria física.

Nosso objetivo é, após tratamento, transformar os dados de localização em uma versão ilegível dos originais, para que ainda possam ser utilizados como a prova de conhecimento zero, mas não podem ser lidos sem uma chave de criptografia, ou, em certos casos, de forma alguma. Outras técnicas que usamos incluem uma estrutura de conjunto probabilística, privacidade diferencial e k-anonimato, aproximando os dados de uma anonimização completa.

Os dados coletados pela Inloco para oferecer seus serviços vêm do dispositivo móvel através de nosso Software Development Kit (SDK). Cada aplicativo deve apresentar para seus usuários a Política de Privacidade da Inloco em seus próprios Termos e Condições de Uso e Políticas de Privacidade, informando que os dados serão coletados pela Inloco. Uma vez autorizado, nosso SDK começa a coletar os dados sem identificar os usuários. Os usuários também podem negar a coleta de dados optando por não permitir e não dando consentimento, o que desativa os recursos para eles. Além disso, cada aplicativo deve permitir que os usuários optem por não coletar os dados a qualquer momento, dando aos usuários a propriedade de seus dados.

A equipe da Inloco compreende o poder e a sensibilidade dos dados de localização e é por isso que temos um compromisso interno de ir muito além para manter a proteção da privacidade do usuário.

Peça uma demonstração: contato@incognia.com
Saiba mais: www.incognia.com/pt