ForgeRock®

Differentiating Through Customer Experiences in Insurance

A Guide To Enabling Modern Digital Identity | Part 1

The Shifting Insurance Landscape

Insurance is transforming from its low-interaction roots into a high-touch, multi-channel distribution industry. The ability to deliver seamless, secure, and scalable digital experiences that span the customer journey is no longer a nice-to-have feature. Research from **Kubra** shows that as many as 46% of U.S. consumers see experiences as a top priority when selecting an insurance provider.

It's no secret that leading retail banking, wealth management, and fintech providers have reaped benefits by investing time, effort, and money in reimagining how customers interact with their brands. While a similar trend has emerged in insurance, most of the industry has struggled to keep pace with changing customer expectations. It's therefore no surprise that 60% of insurance providers surveyed by the **IBM Institute of Business Value** have admitted to the lack of a customer experience strategy.

The rapidly changing macroeconomic climate has pressured insurance providers to revisit their approach to innovation, forcing them to either build capability in-house or acquire innovation through a merger-and-acquisition (M&A) strategy. Those leading the pack have sought to widen distribution reach through third-party partners, grow their secure application programming interface (API) capabilities, minimize their risk-premium spreads through usage-based insurance (UBI), and reinvent their claims processes.

However, maximizing ROI on embedded insurance across an industry ecosystem is no easy feat, especially given:

- The emergence of new ecosystem stakeholders, such as third-party service providers, internet-of-things (IoT) technology providers, platform orchestrators, and point-of-sale (POS) brokers, beyond the traditional provider, customer, and broker;
- The fragmented view of customer needs across multiple channels of customer engagement including first- and third-party customer touchpoints, mobile apps, web apps, and call-center interactions;
- The growing risks posed by persistent cyberthreat networks, including well-funded crime syndicates and rogue-state actors, resulting in exponential growth in account takeover (ATO) attacks, unauthorized access, and elaborate attack vectors such as multi-factor authentication (MFA) prompt bombing;
- The continued challenges with interoperability, security, and scalability posed by legacy identity and access management (IAM) infrastructure, which inhibit digital agility and continuous implementation/deployment (CI/CD), driving up total cost of ownership (TCO) and constraining digital innovation.

The ForgeRock Identity Platform provides a comprehensive set of converged capabilities for addressing these problems, thereby enabling insurance providers to:

- Differentiate through customer experiences
- Drive profitability
- Accelerate digital agility

About the "Differentiate Through Customer Experience in Insurance" Series

The "differentiate through customer experience in insurance" series consists of three business-focused guides that break down the end-to-end customer journey and offer a view of how providers can evolve their customer experiences using the comprehensive capabilities of the ForgeRock Identity Platform:

1

Guide 1 focuses on the search-and-quote, registration and login, and self-service customer journey experiences

2

Guide 2 focuses on purchase, claim, and usage-based insurance customer journey experiences

3

Guide 3 focuses on ways in which modern IAM mitigates the risk of fraud and unauthorized access, while enabling digital agility and ecosystem expansion

Each guide will use a hypothetical persona to map out flows, pain points, and opportunities across a typical "current experience" journey, before painting a picture of what the "enhanced experience" journey could look like when enabled by the comprehensive features of the ForgeRock Identity Platform. Each guide will also offer some practical steps for insurers to consider when moving forward with their IAM modernization.

The Insurance User Journey

A typical insurance user journey consists of five stages, each presenting challenges and opportunities for acquiring customers, converting sales, and driving up-sell. Leading insurance providers invest significant time, effort, and money in improving customer experiences across each of these stages, but very few are able to elevate both experiences and security without some compromise. The ForgeRock Identity Platform provides the capabilities needed to achieve both of these objectives, while helping insurers achieve compliance, reduce TCO, and accelerate digital agility.

A Typical User Persona

The ability to deliver seamless, secure, and scalable customer experiences is largely shaped by the degree to which providers can infuse a user-centered design (UCD) approach into their digital strategy and CI/CD lifecycle. Developing credible user personas through ethnographic research and product release user testing is at the core of this thinking. This guide will adopt the hypothetical persona illustrated by figure 1.

Age: 34
Job: Digital Marketing Mgr.
Children: 4-year-old son
Status: Single
Education: Degree
Archetype: Ruler

Grace

"Finding enough time to do all I need at work and at home is challenging enough without having to deal with avoidable problems."

"Give me the tools and I will do as much as I can myself."

"It's time I started planning for my future and my son's — the party days are over!"

Goals:

- Nurture a happy home environment
- Advance professionally
- Achieve and sustain financial well-being

Challenges, Fears, Problems:

- Inability to balance all priorities in life
- Not being able to sustain long-term debt
- Financial hardship caused by economic downturn or illness

Buying Needs:

- Protect new home and property with adequate insurance
- Maximize disposable income

Buying Decision Process:

- Does this fit my needs?
- Am I getting good value?
- Can I get it done quickly?

Figure 1. Hypothetical insurance persona

Practical steps to consider:

- [ ] Map out all touchpoints between a persona and the services they are interacting with.
- [ ] Gain insight into how a persona interacts with brand and advertising.
- [ ] Develop an understanding of the core fear and frustration triggers that are driving decisions.
- [ ] Drill into the online and offline tools the persona uses to research potential purchases.
- [ ] Develop an understanding of factors driving the persona to abandon an experience.
- [ ] Gain insight into any accessibility challenges facing the persona.

USER JOURNEY STAGE 1:

Search-and-Quote Experience

The search-and-quote experience is critical to helping insurance providers acquire new customers. The move from brick-and-mortar settings to digital channels makes it critically important for insurers to reduce unnecessary friction and waiting time for quote loads. The returned results must also match the prospective customers' known (and at times, unknown) needs.

The search-and-quote experience provides insurers with an opportunity to widen their distribution channels beyond the conventional first-party POS touchpoint: the insurer website. Innovative insurers with well-established partner ecosystems provide customers with a wide range of third-party POS touchpoints where they can purchase their offerings. These may include price comparison sites, retail shopping sites offering insurance on high-value items, travel sites offering travel insurance, and open finance sites where providers from the wider financial ecosystem (such as a retail bank) offer personalized value-added services.

Current Experience: Persona Journey

When Grace, our hypothetical insurance persona, engages with an insurance search-and-quote experience using legacy IAM, she is likely to encounter a standard flow (see figure 2). A busy individual, Grace spots a targeted or organic advertisement online, promoting a bundled home insurance plan for her recently purchased property. Grace is drawn to the advertisement and decides to click the link to find out more. She is then presented with a choice of engagement channels, including a mobile app download, a web app experience, or a call with a broker. She decides to use the web app and completes 20 form fields with her basic information. After pressing search, Grace is presented with a lengthy list of quotes before being distracted by her son and having to shut the laptop for the day.

The next day, while on her lunch break, Grace remembers the 10 minutes she spent searching for the quote and decides to download the provider's mobile app to revisit the search. After a three-minute download, Grace is prompted to enter her basic details and search parameters again. She completes the 20 form fields and is provided with a lengthy list of quotes. The search results do not appear to match her needs and fail to take her recent home purchase into account. Grace begins to lose faith in the process and decides to shut the mobile app to enjoy her remaining lunch break.

Two days later, while rushing from one meeting to the next, Grace receives a call from a sales agent following up from her online search. The agent asks her to confirm her identity and her main search parameters. Grace doesn't have time, so she thanks the agent and terminates the call.

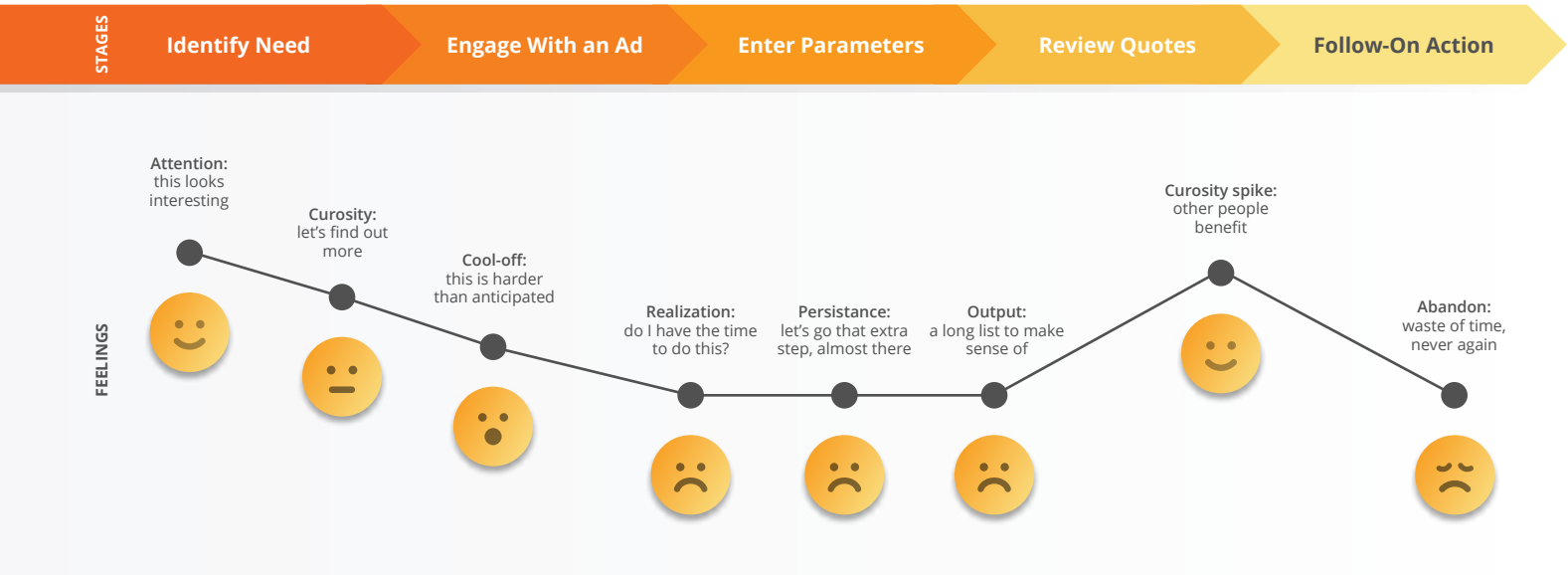

Figure 2. A standard search-and-quote experience

Current Experience: Underlying Identity Challenges

- **Too many form fills**: Grace is frustrated about having to provide all her personal information before being presented with a list of quotes. Grace is even more frustrated about having to enter the information twice; first with the website and again when she engages with the mobile app. This frustration leads her to abandon the search-and-quote experience. The insurance provider loses a potential customer and any associated revenue.

- **Failure to recognize a known prospect**: Grace responded to targeted online advertising as she recalls buying auto insurance from the same provider some years back. She was expecting this provider to have some knowledge of who she is and what her needs might be. Unfortunately, her experience with both the web and mobile app have made her think that the provider doesn't recognize her as a former customer.

- **Lack of single view of needs**: Grace is also frustrated with the fragmented experience across the insurer's website and mobile app. Grace couldn't understand why, having provided her personal information on the website, she was asked to rekey this information on the mobile app. She can't understand why the insurer couldn't re-use this information to better understand her needs.

- **Lack of third-party integration at POS**: Grace recalls completing her online mortgage application for her recent house purchase, remembering the home insurance quotes she was provided at POS. She found these appealing, but didn't have time to complete the quote process at that time. She is surprised that the insurance provider she recently engaged with wasn't on this list, causing her to question whether it's a credible provider.

Enhanced Experience: Identity Enablers

When Grace engages with the future-state search-and-quote experience enabled by the ForgeRock Identity Platform, she encounters a seamless experience that significantly increases the probability of her purchasing a home insurance policy at the first or second touch (see figure 3). ForgeRock helped the provider:

- **Reduce form fills and recognize a known prospect**: Grace is satisfied with her search-and-quote experience. Because she only needed to complete five form fields on her visit to the website, she was willing to complete two more form fields on her second touch via the provider's mobile app.

> ForgeRock **Progressive Profiling** capabilities helped the insurer use the information entered in both touchpoints to enrich historical information on her as a prospect held in the insurer's customer relationship management (CRM) system, and to provide a personalized offering.

- **Build a real-time view of needs**: Grace is happy that the provider recognized her recent property purchase and the imminent expiration of her auto insurance.

> The ForgeRock **Identity Management** and **Identity Synchronization & Reconciliation** capabilities helped the insurer initiate a secure API call to an open finance data aggregator and the driving authority to establish that she is both a mortgage owner as well as a licensed driver. These data points helped the provider build a picture of needs, and personalize offerings to fit with these.

- **Leverage third-party integration at POS**: Grace was informed by the provider that her home insurance policy could be re-quoted by her online broker when she came to renew her mortgage in two years, ensuring she could continue to benefit from best offers available without having to go through the search-and-quote experience.

The ForgeRock **Identity Management** and **Identity Gateway** capabilities helped the insurer secure the API traffic with third-party providers, such as price comparison sites, retailers, and other financial service providers, enabling personalization at POS.

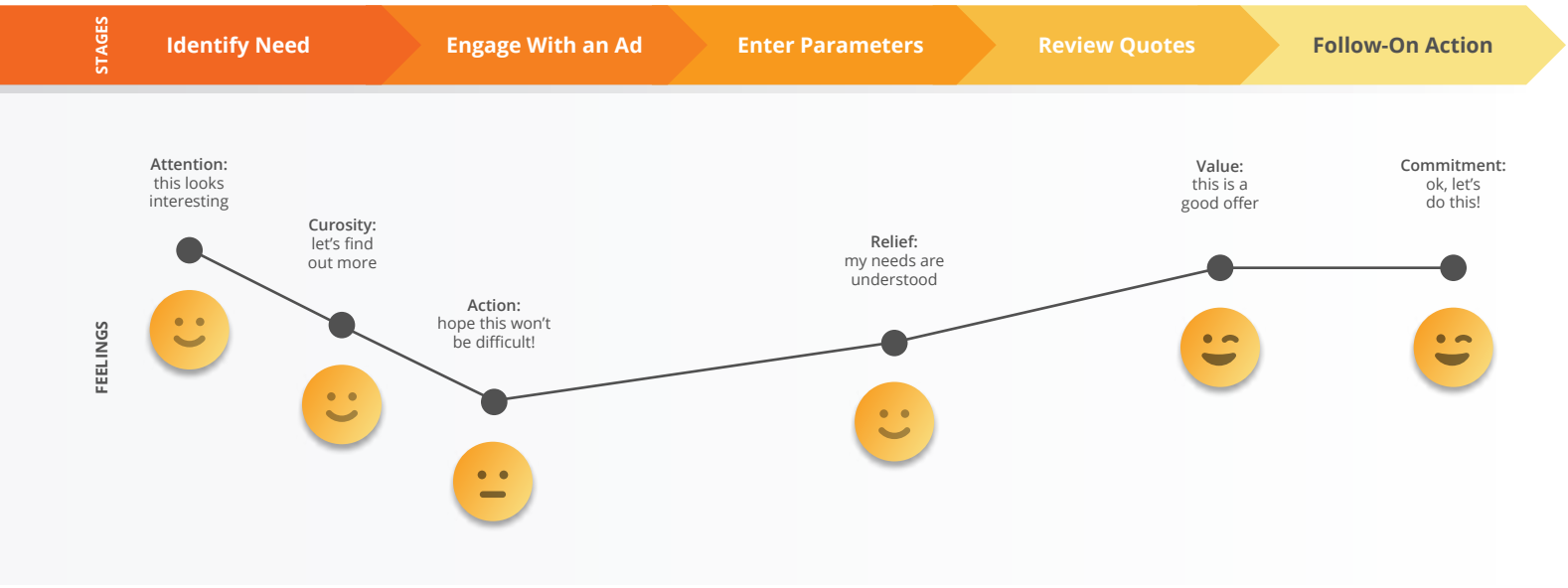

Figure 3. An enhanced search-and-quote experience

Practical steps to consider:

- [ ] Understand the relationship between form fills and customer abandonment.
- [ ] Run A/B tests on progressive profiling deployments to optimize conversions across the first two touchpoints.
- [ ] Map out open and premium APIs made available within the third-party ecosystem.
- [ ] Map out data available within the third-party ecosystem to define opportunities for multi-channel distribution.
- [ ] Ensure your CRM strategy allows you (within the constraints of privacy regulations) to retain data on historical prospects, and use this to turn "unknown" prospects into "known" customers as early as possible.
- [ ] Work toward ensuring customers have a consistent experience across your website and mobile apps.

PROOF POINT

Research from **Formstack** shows that limiting form fields to four (or fewer) can increase conversions by up to 160%

USER JOURNEY STAGE 2:

Registration and Login Experience

Registration and login experiences are a critical ingredient of an effective insurance journey. Consumers expect to be able to perform their know-your-customer (KYC) and anti-money laundering (AML) checks quickly to complete their registration in minutes, not hours or days. Those very consumers also expect their registration and login experiences to be seamless across all web, mobile, call center, and third-party channels.

At the same time, consumers expect their insurance providers to secure their personal data and take all necessary measures to protect them from the common attacks, such as account takeover (ATO). Any additional friction introduced to protect them at both the identity proofing and login stages needs to carefully balance experience and security. Leading insurers recognize that a bad registration process significantly increases the risk of fraud. They also recognize that a poor password-based or static multi-factor authentication (MFA) experience can lead to customer abandonment and regulatory breaches.

Current Experience: Persona Journey

When Grace, our hypothetical insurance persona, engages with a standard registration and login experience delivered through legacy IAM infrastructure, she will encounter a typical flow (see figure 4). As someone who aims for efficiency, Grace is eager to ensure that any identity proofing checks are carried out quickly. Grace would never agree to go through the paper proofing exercise she recently endured when completing her mortgage. She is happy to authorize providers to use existing identification records, biometrics, and alternative identity verifiers to ensure she can clear registration hurdles as quickly as possible.

Grace is prompted to enter her driver's license details, upload a picture of it via the web portal, and then provide an electronic copy of her proof of property purchase by email. Much to her frustration, the provider's mobile app does not provide this functionality and she postpones completing the process until later that evening. Once back at her laptop, Grace completes 10 form fields to enter her driver's license details, takes a picture of the license, and transmits it to her laptop for uploading to the provider's web portal. She then searches for an electronic version of her property purchase confirmation, but can only locate the hardcopy, which she scans with her mobile phone and sends off to the designated email address. The second touch interaction lasts 15 minutes.

Once fully registered, Grace is asked to set up a password, provide answers to five memorable questions, and accept a one-time password (OTP) sent to her mobile phone via text message (SMS) to verify her identity. She waits for five minutes but does not receive an OTP, and is unable to log in. Grace places a call to the call center and waits 12 minutes to have her registration profile successfully reset. Two days later, Grace is eager to review her insurance documentation and attempts to log in via the provider's mobile app. She forgets her password, completes a "change password" request, and receives an email link to complete the process, prompting her to verify her identity via another SMS OTP. The next day, she starts receiving suspicious SMS messages from an unrecognized number and begins to suspect that the insurer is not doing all it can to protect her data from malicious actors.

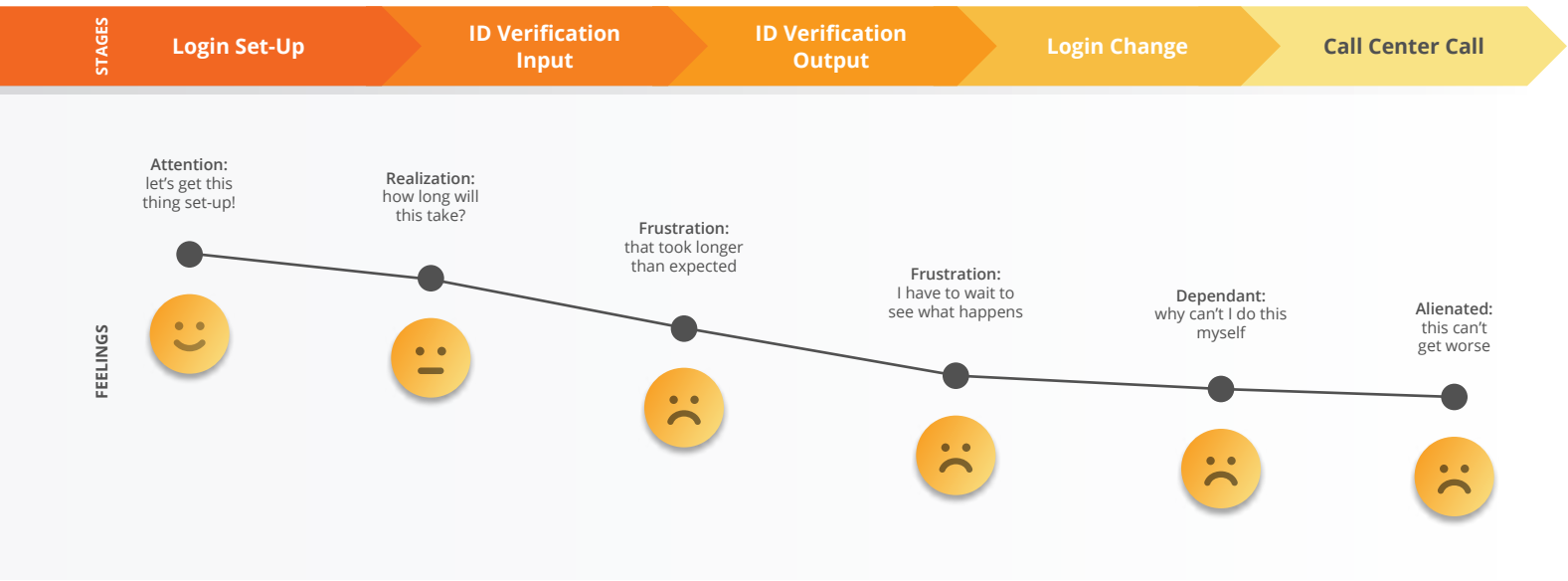

Figure 4. A standard registration and login experience

Current Experience: Underlying Identity Challenges

- **Fragmented identity proofing**: Grace is frustrated by the amount of time it has taken her to complete eKYC and AML checks. By delaying the outcome of the identity proofing process, the insurer made Grace feel anxious and prompted her to question whether she went with the right provider. When asked to give a Net Promoter Score (NPS), Grace rates the provider at five out of 10 ("detractor").

- **Lack of an omnichannel experience**: Grace was anticipating a consistent identity proofing experience across the web, mobile, and call center channels. But the inconsistency she experienced prompted her to question whether the insurer can serve her needs in an effective and prompt manner before the policy even came into force.

- **Potential phishing attack**: Grace was concerned by the receipt of a series of suspicious SMS messages soliciting her with attractive insurance offers only a day after having set up her account with the insurance provider. Grace spotted these as possible phishing attacks and deleted the messages, but she was compelled to revisit the eight-character password she set up at registration, and questioned whether her personal data was being protected by the insurer.

- **Password-based friction and risk**: It took three attempts for Grace to set up a password that met the complexity parameters set by the insurer at registration. She then had to reset her password following a suspected phishing attempt. Grace is prompted to enter her password every time she wishes to access basic policy information, and struggles to remember it when accessing the service through her laptop.

Enhanced Experience: Identity Enablers

When Grace engages with registration and login enabled by the ForgeRock Identity Platform, she encounters a seamless, secure, and adaptive experience (see figure 5), thereby significantly driving her positive perception of her insurer. ForgeRock helped the provider to:

- **Leverage third-party eKYC capabilities**: Grace is relieved to complete the eKYC and AML checks in minutes by being given the option to use a biometric third-party tool built into her registration experience to verify her identity. Grace is also relieved that she can authorize the insurance provider to confirm her recent home purchase via her mortgage provider.

The ForgeRock **Trust Network** gave the insurer access to an extensive library of pre-built identity proofing capabilities that were orchestrated using the ForgeRock **Intelligent Access** no-code orchestration engine. As a result of her seamless, secure, and rapid registration experience, Grace provided an NPS rating of 8 out of 10.

- **Enable omnichannel registration and login experiences**: Grace is pleased with her registration and login experience across the provider's mobile app and web portal. Both gave her the ability to leverage the biometric third-party identity verification tools and provided access to passwordless login.

  The ForgeRock **Mobile SDK** (software development kit) gave the insurer the ability to seamlessly integrate the end-to-end identity journey into the mobile app design, ensuring that Grace had a consistent journey across all channels.

- **Mitigate ATO attack risks**: Grace is pleased to know that her insurance provider takes all the necessary steps to protect her personal data. At registration, Grace was asked to verify her identity using a biometric third-party tool that was easy to use. She also noticed that she was asked to complete a strong factor authentication (SCA) check while attempting to log in to her web portal through her work-based desktop machine.

  ForgeRock **Autonomous Access** gave the insurer the ability to use artificial intelligence (AI)-driven identity to identify anomalous access requests and introduce the appropriate amount of friction to protect Grace's data.

- **Enable passwordless login**: Grace is relieved that she can avoid using passwords to access basic aspects of her insurance policy. While using the provider's mobile app, Grace is prompted to use her fingerprint biometric to view her insurance documents. She is also pleased to know that changing her payment methods prompts an automatic SCA check to prevent malicious actors from getting access to her policy.

  ForgeRock **Passwordless** capabilities gave the insurer the ability to leverage FIDO2 passwordless standards, including **passkeys**. Passwordless journeys are rapidly built via the ForgeRock Intelligent Access no-code orchestration tools, allowing Grace to avoid interacting with passwords while logging into the mobile app and web portal.

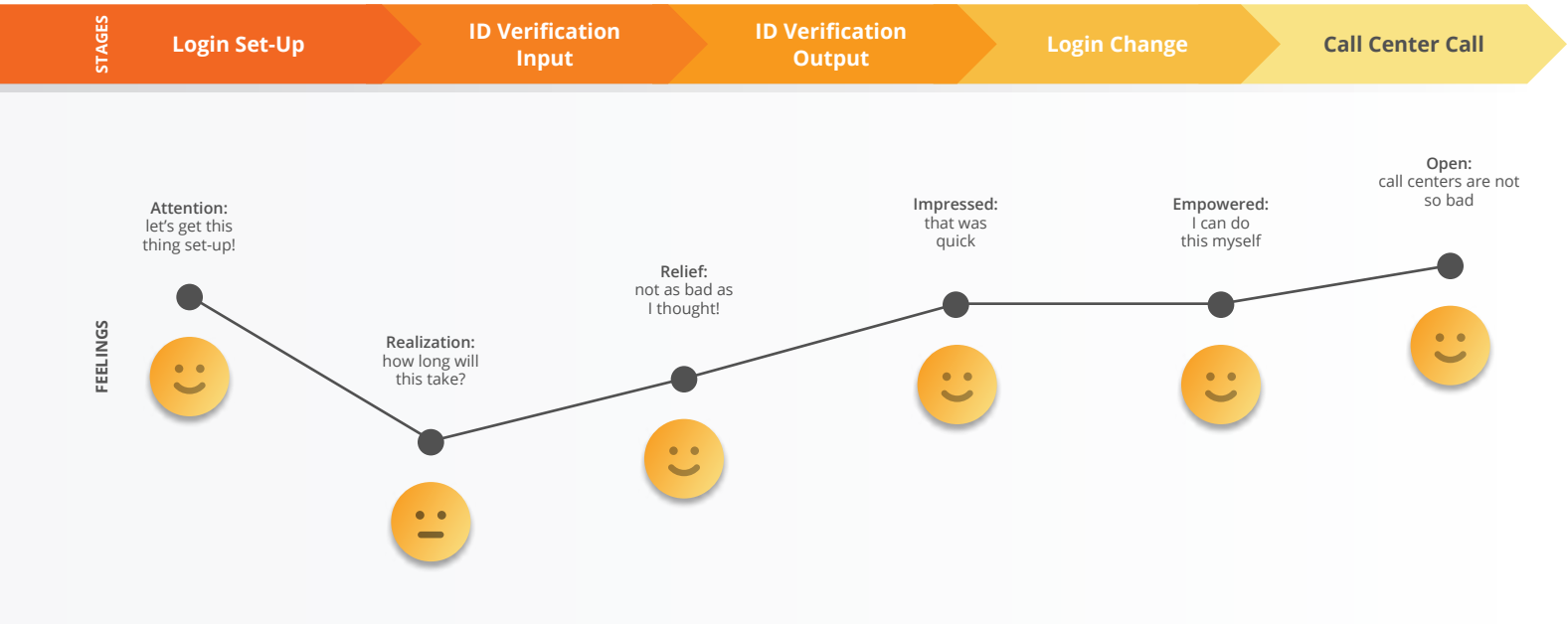

Figure 5. An enhanced registration and login experience

Practical steps to consider:

- [ ] Map out third-party identity proofing tools that can significantly reduce friction at the eKYC and AML proofing stages.
- [ ] Draw continuous insights from uptake of eKYC and AML proofing tools — are these the right for your customers?
- [ ] Ensure your web apps/portals and mobile apps are not developed in isolation, giving customers consistency and predictability every time they log in and/or want to authorize a change.
- [ ] Understand and leverage access signals as widely as possible, and use these to automate threat detection and protection.
- [ ] Give your customers the choice to authenticate with passwordless technologies and make it easy for them to enroll credentials and devices.
- [ ] Ensure you build comprehensive and user-friendly step-up logic into your access journeys based on contextual risk.

PROOF POINT

ForgeRock helped a major retailer leverage improvements in login experiences to drive a 60% increase in online orders.

ForgeRock helped Mox Bank reduce onboarding to just **180 seconds**.

USER JOURNEY STAGE 3:

Self-Service Experience

Traditional insurance services were delivered through in-person broker interactions and call centers. Despite the rapid development of digital banking, lending, and wealth management, most non-digitally native insurers offered their customers limited web- and mobile-based features to control their password and consent settings, placing the onus on the customer to engage regularly with call centers.

The COVID-19 pandemic significantly increased the strain on call center operations and costs. Leading insurers soon started to follow the major retail banks by developing web- and mobile-based features to enable and accelerate self-service, significantly reducing the touchpoints between call centers and customers. Offering customers intuitive tools for self-service not only reduces operating costs, but also delivers a streamlined and secure method for customers to control their policies, thus helping to build long-term trust and loyalty.

Current Experience: Persona Journey

When Grace engages with the provider's insurance app and website powered by legacy IAM (see figure 6), she is surprised to learn that the provider offers limited self-service capabilities, instead pushing her to the call center. Grace isn't happy about being forced to log in with passwords and having to use SMS OTPs to verify her identity, given her poor experience with the latter during the registration process.

In addition, Grace is uncomfortable with her personal data being shared with third parties without her ability to control the process. She feels this should be done on a case-by-case basis and controlled by the data subject. This was an important reason in her choice to go with her purchase, given the insurer's bold claims to protecting customer data in the advertisement she originally engaged with. She now feels like she's been misled, since neither the provider's mobile app nor the web portal give her any controls to manage data sharing consent.

Grace decides to contact the insurer's call center to discuss her observations and to determine if the provider can give her an alternative means to self-service in the future. After a 15-minute wait, Grace is asked to confirm her personal information as part of security checks. She is then asked to provide an answer to one of the secret questions she set up at registration that she cannot remember, forcing her to revert to her onboarding emails. After several minutes, she clears the security checks only to be told that the provider is only able to offer password login and SMS OTP verification.

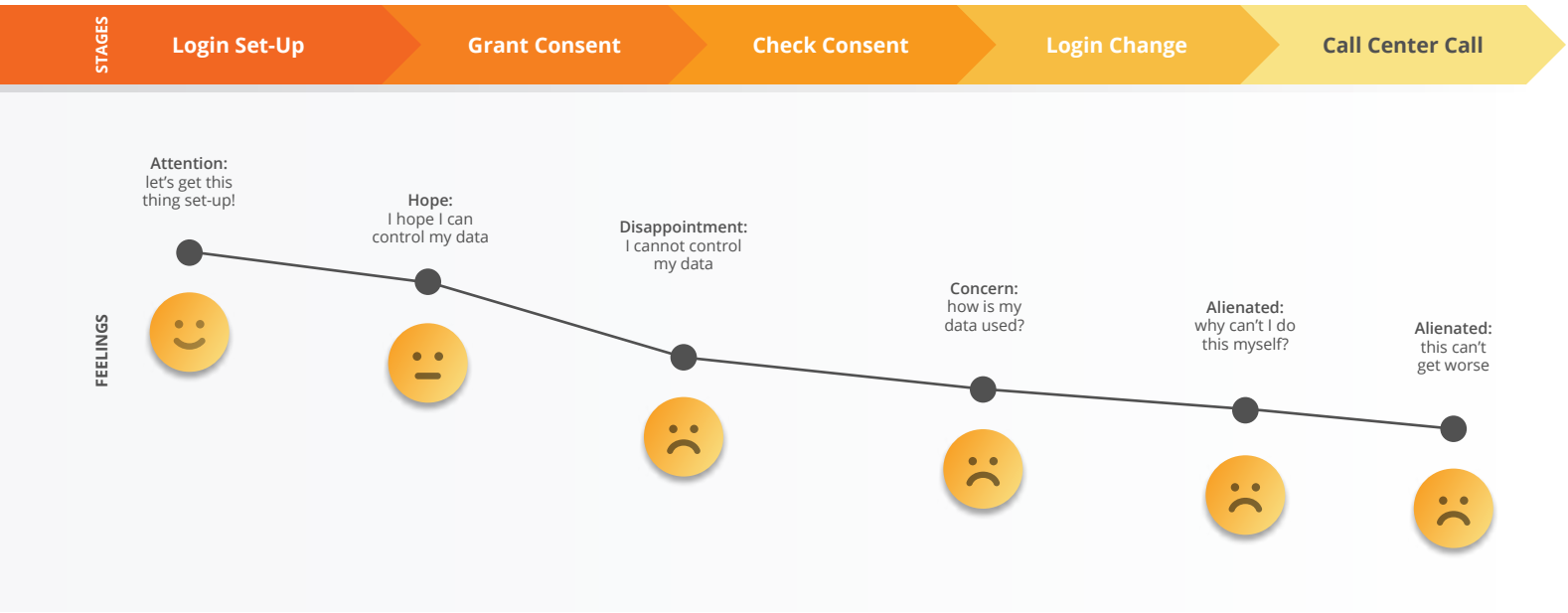

Figure 6. A standard self-service experience

Current Experience: Underlying Identity Challenges

- **Lack of login self-service**: Grace is frustrated with the inability to configure her own login preferences and having to engage with the call center to resolve basic problems. The insurance provider has recognized that 24% of all inbound calls relate to login tickets, but cannot offer login self-service due to its legacy infrastructure.

- **Absence of consent controls**: Grace feels she has no control over how her personal data is shared with third parties. She is concerned that the provider may be breaching the General Data Protection Regulation (GDPR) requirements. She knows that the provider uses her data to deliver up-sell promotions from the provider network, so she is sure that her data, one way or another, is being shared without her consent. This knowledge shatters the trust in her provider, causing her to doubt whether she'll renew the policy.

- **Bad call center verification experience**: Grace spends no less than 15 minutes on a call every time she contacts the call center. A third of that time is spent verifying her identity. The provider doesn't have the ability to verify callers' identity any other way, and has been subject to damaging identity fraud attacks.

- **Limited choice of login and authorization credentials**: Grace was hoping that her insurance provider would offer an experience similar to that of her mortgage provider — the ability to select from a variety of identity providers, including credible social identity providers. She was also hoping to have the ability to enable her mobile biometrics to simplify the login and verification process.

Enhanced Experience: Identity Enablers

When Grace engages with the self-service experience (see figure 7) enabled by the ForgeRock Identity Platform, she is given the tools to personalize her password and consent settings, thereby significantly reducing her need to engage with the call center. ForgeRock helped the provider to:

- **Enable login self-service**: Grace is pleased to have the ability to easily reset her passwords and change her personal information via the provider's mobile app and web portal. Self-service reduces the need for her to use the call center.

> ForgeRock Identity Management capabilities give insurers the tools to implement **login self-service** across mobile and web touchpoints, significantly reducing operational overhead and costs associated with managing login-related queries through the call center, while enhancing Grace's experience.

- **Provide consent-controls**: Grace is pleased to have the ability to control who her personal data is shared with. Grace can revoke permissions from third parties as she pleases, so she feels that she can trust her insurance provider for the long term.

> ForgeRock **consent management and privacy** capabilities give Grace the ability to control who her data is shared with and to revoke access at will, while helping the provider ensure it complies with local privacy regulations. These capabilities also help to build a long-term relationship with Grace that introduces opportunities to increase her average product holding.

- **Streamline call-center verification**: When engaging with the provider's call center, Grace only needs to accept a push notification sent via the provider's mobile app to verify her identity. This reduces friction when she contacts the call center. Grace feels that she can engage more effectively with the provider across all mobile, web, and call center channels.

  ForgeRock **Access Management** capabilities allow the provider to leverage standards-based identity federation and **Client Initiated Backchannel Authentication** (CIBA) to perform secure identity verification checks in a fraction of the time spent conducting verbal security checks.

- **Provide choice of login and authorization credentials**: Grace is able to use the login self-service features built into the provider's mobile app and web portal interface to select from a wide range of identity providers, enrolled biometrics, and devices to simply log in and to authorize material changes and transactions across her policy portfolio. Grace configures these choices to fit with her needs, and takes to social media to speak about how happy she is with this experience.

  ForgeRock **Access Management** capabilities enable Grace to use **social registration** providers, passwordless, and third-party biometrics to elevate her experiences and security across all touchpoints, all enabled by **Intelligent Access** no-code orchestration.

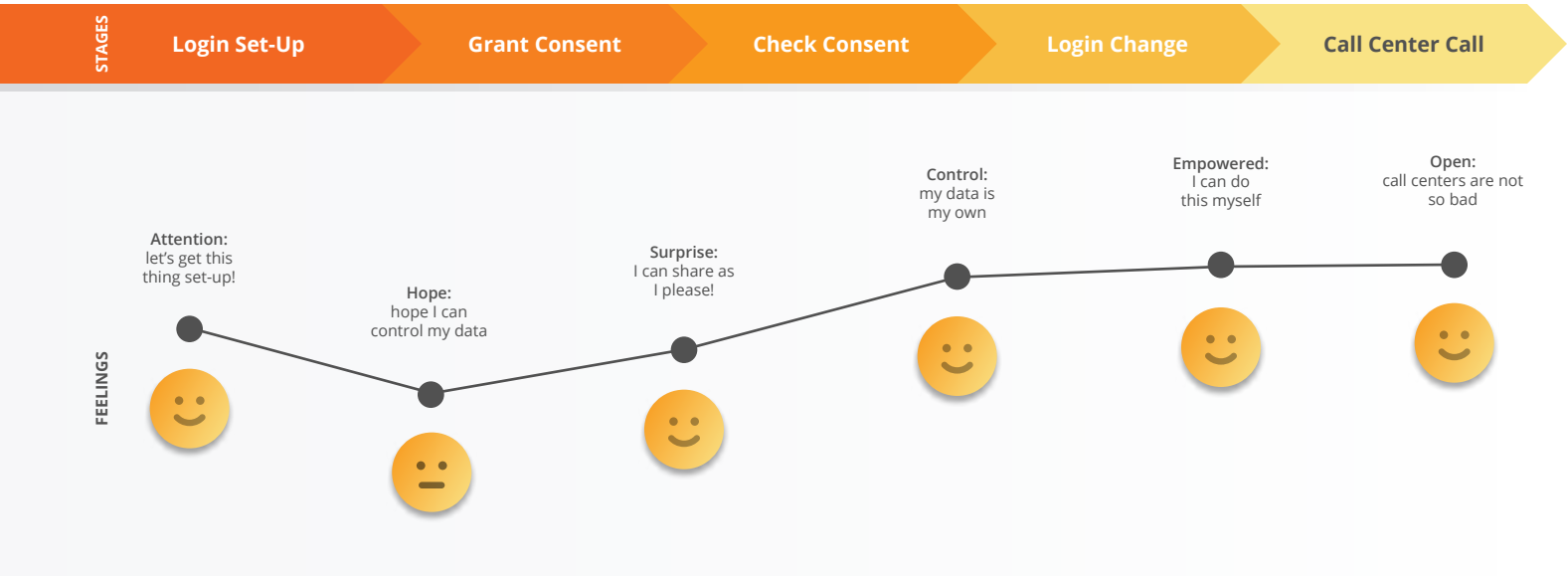

Figure 7. An enhanced self-service experience

Practical steps to consider:

- [ ] Maximize customers' ability to self-serve across the end-to-end customer journey.
- [ ] Give customers the ability to manage data-sharing consent with third parties to enable both marketing and up-sell conversions.
- [ ] Give customers visibility into the third parties they have consented to sharing data with, as well as the controls to revoke access easily.
- [ ] Continuously look for opportunities to remove overhead on call center support, and look to bake these into the mobile apps and web apps.
- [ ] Give customers a wide choice of credentials to login and authorize policy changes, including the ability to delegate access to trusted persons, such as family members and caregivers.

PROOF POINT | ForgeRock has helped global enterprises reduce security-related calls into call centers by **40%**.

Summary

The comprehensive capabilities of the ForgeRock Identity Platform help leading insurance providers elevate end-to-end customer experiences and security without compromise. By streamlining how prospects and customers interact with insurers at the search-and-quote, registration and login, and the self-servicing stages of the user journey, modern IAM can reduce abandonment, accelerate conversions, elevate retention, and, ultimately, increase customers' average product holding across all engagement and distribution channels.

Contact us to find out more and be sure to keep a lookout for the next guides in this series.