THE STATE AND FUTURE OF CIAM

ForgeRock

ForgeRock's Alex Laurie on How to Meet Customer – and Regulatory – Expectations

ISMG
INFORMATION SECURITY MEDIA GROUP

FORGEROCK'S ALEX LAURIE ON HOW TO MEET CUSTOMER – AND REGULATORY – EXPECTATIONS

Customer identity and access management – CIAM – is less of an option and more of an expectation as customers and citizens exercise how they wish to be treated by the enterprises with which they conduct digital business. **Alex Laurie** of ForgeRock details the current state and future of CIAM.

In this video interview with Information Security Media Group, Laurie discusses:

- Factors driving the CIAM evolution;
- What customers and citizens now expect;
- What's needed in a modern CIAM solution.

Laurie, who is responsible for the ForgeRock Solution Architecture team globally, has over 20 years of experience in security and identity technology. During this time, they have been involved with digital transformation on both the vendor and system integrator sides, working alongside government departments, the military, multiple police forces and the banking sector. At ForgeRock, they interact on a daily basis with enterprise-scale organizations, supporting clients and partners with their wealth of knowledge in this fast-moving sector.

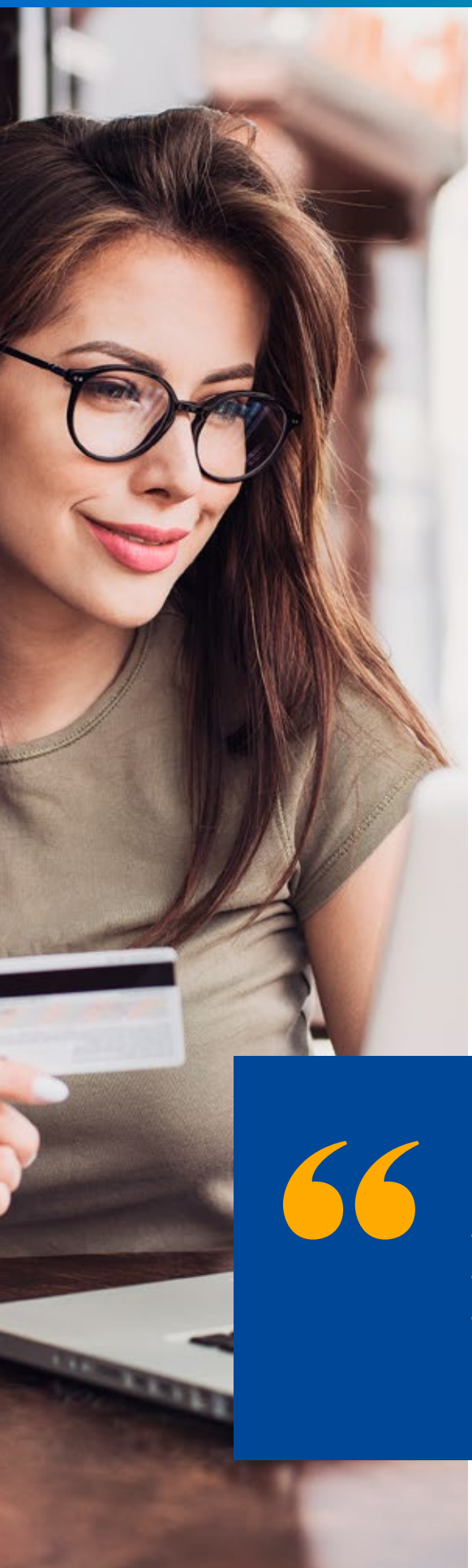
THE STATE OF CIAM TODAY

TOM FIELD: How would you describe the state of customer identity and access management, or CIAM, today?

ALEX LAURIE: There are two conflicting areas when we talk about CIAM. The first is the ongoing and ever-increasing pace of digital transformation, which is happening at pace and across industries we didn't think needed it. But the impact of recent events and pandemics have pushed that forward. There's also the ongoing desire from businesses to modernize, improve their systems and hit their speed to market.

The other side of it is that CIAM, which is very much a broadcast, large-volume interaction between you and your end users – your end consumers or citizens –historically was developed on homegrown solutions. You also get the scenario where organizations with multibrands or multiservices come in through acquisition. Often, customers or prospects have five or six different CIAM solutions and don't have one way to decide who their customer is and what that customer wants. So it's important. And the drivers behind things like COVID are pushing us forward and trying to make things more impactful for end users – for consumers and citizens.

> "The whole idea of working from home and living at home and shopping at home is pushing this accelerated digital transformation and convergence of the use cases that we've seen around workforce and CIAM, which is pushing us forward."



DRIVERS FOR CIAM

FIELD: What factors are most driving the evolution of CIAM today?

LAURIE: It's about customer expectations and the end user's needs. It's very common now for consumers to shop with their feet – or in this case, with their mobile phone. We're also seeing the drivers where people had to work from home and couldn't go out. And that's starting to become a problem, but during COVID it became a real problem at the peak. I still think we have areas in the world where people are still stuck at home. The whole idea of working from home and living at home and shopping at home is pushing this accelerated digital transformation and convergence of the use cases that we've seen around workforce and CIAM, which is pushing us forward. Also, the indications around the market and the end users are pushing us to be better, to be faster, to get a service to market quicker and to deliver something of value as quickly as possible without making it as painful as possible.

> "Historically, when you looked at a consumer interaction with the business, it was about, 'Does the business trust the user to do the thing they're trying to do?' Now we also have, 'Does the user trust the business to look after their data and manage it and use it appropriately?'"

CUSTOMER/CITIZEN EXPECTATIONS

FIELD: You talk about the customer expectations or citizen expectations. What are they today? Are they that you, a business, will recognize me as Amazon or as Netflix does?

LAURIE: We now have this expectation driven by these fantastic services. It starts with our Apple or Android devices, which are Google and Apple. They know us. They know more about us, probably, than we know about ourselves, and the experiences we have on those devices make life easier for us. The app-led development process has driven this end-user experience to push us further and further. Our generation of security experts grew up with green screens and very complex logins and just painful processes. The generations coming up behind us are experiencing login as just, "Here's my face. I'm into a service." That is driving the end user expectations from the experience perspective. And from a corporate perspective, the employees want that experience as well. So we have that convergence of an employee, a citizen, a customer or consumer – someone just doing their job – wanting things to be as easy as possible. That is the most important driver.

The other driver is that people are building their awareness around privacy and the idea that, "My data is my data. I'm letting you have it." There's an interaction between a brand or a service and the end user, and there's knowledge of, "This is what I'm doing with my data or you're doing with my data. And I give you permission because it has value to me." People are starting to interact with brands. They understand that the first-party relationship between them and their customer or consumer or citizen is vitally important and that trust and privacy of data are important – again, driving that expectation.

> "Our generation of security experts grew up with green screens and very complex logins ... The generations coming up behind us are experiencing login as just, "Here's my face. I'm into a service." That is driving the end user expectations from the experience perspective."

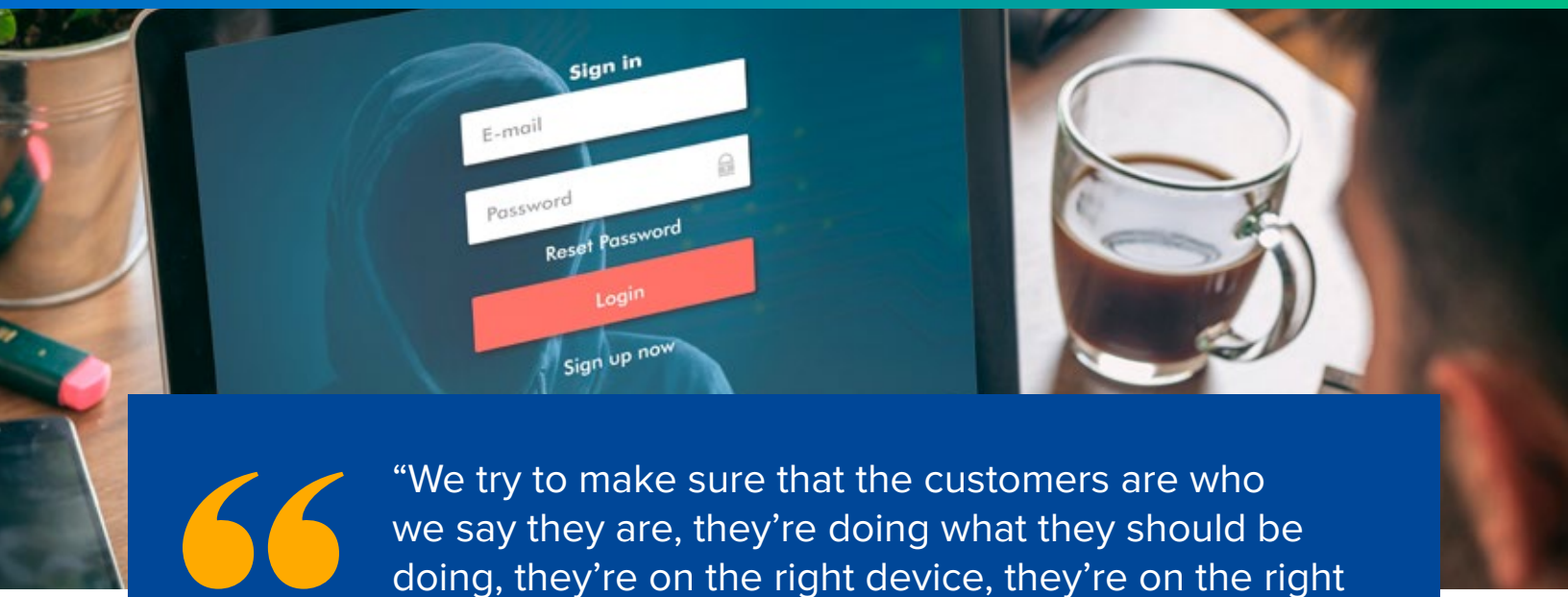
CIAM SOLUTION REQUIREMENTS

FIELD: Given these factors and expectations, what is required in a CIAM solution?

LAURIE: We can talk about it in a very simple, linear process flow and then realize it always loops back and there's always repetition. The customer or citizen onboarding has to be as simple as possible. In a citizen world, we want to be able to use the existing citizen identity providers, or IdPs – the services that prove your identity at a government level and get you in as quickly as possible to access the service you need. And from a consumer perspective, it's about using something that you already have to get in and get access without having to fill in a 55-page form to buy a pair of skinny jeans. Different generations of users have different expectations, but the whole onboarding registration piece has to be as easy as possible.

And the level of assurance of that needs to be managed, depending on how important the services is. There are different levels of assurance for banking, shopping or getting a new driver's license. Once you're in, then it's about the ability to do self-service – manage your profile, password or any interactions around privacy and data. And updating the system as easily as possible without having to phone someone is the next core area. Especially when it comes to continuous interactions, it's about how you're building the profile and knowledge about the end user. You've got to do that with consent, with permission, and letting them manage that is very important.

When it comes to daily use or infrequent use, depending on the type of system, it's got to be as easy as, "Here's my face. I'm logging in." You can use modern automations in terms of AI and ML to get in front of the login to protect the users and trust that you know who they are before you get to the username, password or passwordless flow. You need to know that you know the person accessing the system and that you know they're doing the right thing, especially when it comes to more high-profile services, like banking. The other side of it is ease of use. Ease of use doesn't just mean making it invisible. The users need to feel like they're being guided on a journey and doing things in a proper way.



> “We try to make sure that the customers are who we say they are, they’re doing what they should be doing, they’re on the right device, they’re on the right network, and they aren’t a bot or someone trying to maliciously log in. Building that context is important.”

THE RIGHT AMOUNT OF FRICTION

FIELD: When we talk about ease of use, often we talk about friction as well. As you know, the goal is not to eliminate friction. You need an amount of it. But what is just enough friction to be able to meet the needs of nterprise and the customer or citizen as well?

LAURIE: The trust angle goes both ways. Historically, when you looked at a consumer interaction with the business, it was about, “Does the business trust the users to do the thing they’re trying to do?” Now we also have, “Do the users trust the business to look after their data and manage it and use it appropriately?” Sometimes, for example, if I’m just paying 45 pounds to a house cleaner to come and clean my house, then we don’t need to worry about having a step-up transaction.

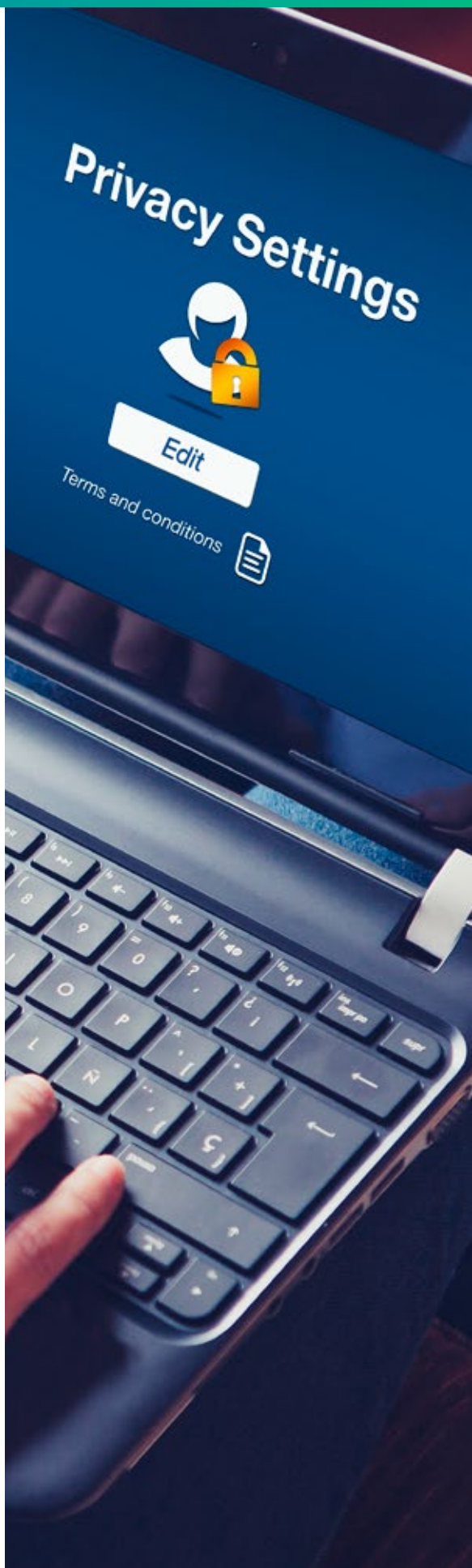
But, for example, if I need to move a lot of money, then obviously there are rules and regulations. Yet I also want to know that the bank actually cares about me moving money and says, “OK, at this point, we need you to type in your password again or do a face ID, or we’re going to gather a whole bunch of contextual signals about you, test them and then make sure you are doing something that’s appropriate and let you know that we are testing this.” That reassures me as an end user that I can trust this organization to handle my data, my information and potentially my money appropriately and put just enough friction in place. And again, it’s very contextual.

CIAM AND REGULATIONS

FIELD: As you've referenced, we've got a shifting regulatory landscape, particularly in terms of privacy. How does one align CIAM with this shifting landscape?

LAURIE: You have to understand where your end users are. Typically, most businesses in the consumer or citizen space tend to operate in defined territories but maybe across multiple territories. So in that environment, you have to be very aware. For example, "We're in Germany; we have to have the data located in Germany. We're in Brazil; we have to have the data located in Brazil." Now, it could be the same company and the same service, but the user data has to be managed separately. That's the very first thing. Understanding how you can segregate data and apply local regulations, rules and protection for your end users in each location is very important.

The second thing is: There are regulations that are very much either transaction-based or purely security-based or even just absolutely the law. For example, the step-up transaction for adding a new payee in PSD2 is mandated by law, but you have to be aware and understand where those are impacted. And sometimes from a CIAM perspective, we may have users who live in a different country but their financial transaction, for example, may be happening where you're based. You have to understand what rules apply in country A and country B. CIAM solutions need to be flexible enough and capable enough to deliver both sides of that argument together for the end user.



THE FORGEROCK APPROACH

FIELD: How is ForgeRock helping its customers develop an effective approach to CIAM?

LAURIE: In terms of the whole journey, first we look at the very early piece. We recently launched our new Autonomous Access service, which is about building that trust picture before you even try and log in. The idea is that 50% of everything we are trying to work out has happened before you even try and log in. So we try to make sure that the customers are who we say they are, they're doing what they should be doing, they're on the right device, they're on the right network, and they aren't a bot or someone trying to maliciously log in. Building that context is important. And it's a continuous journey, so as the customers continue to interact with the organization, you have to learn and keep building that picture around them.

There is a continuous evolution of how people interact with devices and how we can make that easy. How do we make developers' lives easier to bring security into the product and into their services? Also, our journey around the cloud is very important. We need to make sure the end users are protected, that their data is kept where it should be kept, that we take care of compliance and regulatory issues on behalf of the enterprises and make sure everything's patched and updated, and that we support everyone's general transformational desire to move to the cloud. ForgeRock's CIAM solution is recognized by Gartner's Magic Quadrant. We're a leader in the CIAM space and from that perspective, we are continually evolving and pushing the boundaries of what we can do to make CIAM as strong as possible for our customers and their customers.

ABOUT FORGEROCK

ForgeRock®, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is public, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com** or follow ForgeRock on social media.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io