Banking in the Balance: Security vs. Convenience

IBM Trusteer's Valerie Bradford on How to Assess Digital Identities


Valerie Bradford

As banking institutions of all sizes maximize their digital channels, there is growing tension between the need to prevent fraud and the desire to maintain a frictionless customer experience. IBM Trusteer's **Valerie Bradford** discusses how to defuse this tension.

Bradford, a product marketing director with IBM Trusteer, lays out today's fundamental challenge brought about by banks and nonbank financial entities offering new, attractive services.

"Customers want to log in; they want to initiate transactions, even create new accounts with a really user-friendly experience," Bradford says. "But on the other hand, fraud is really here to stay, and it seems like with every new functionality you introduce, there's the opportunity for fraud."

That leads to real tension, she says. "How do you offer that great customer experience without compromising security, authentication and trust?"

In an interview about overcoming these challenges, Bradford discusses:

- The fundamental tension between security and convenience;
- What's at risk with both fraud and customer retention;
- New ways to transparently assess digital identities.

Bradford is an IBM Security product marketing professional on the Trusteer team. With over 10 years of experience, her career has focused on security technology, fraud prevention and authentication. Prior to joining IBM, she held various roles at Pindrop Security and TransNexus.

TOM FIELD: Valerie, we find that banking institutions today are certainly challenged to establish trust over all the new digital channels they're offering existing and new customers. What do you find to be the fundamental tension inherent in this challenge?

VALERIE BRADFORD: Well, Tom, on the one hand, banks are coming into this new digital world and they're competing both with each other and with other fintech applications to provide this great digital experience for their customers and their potential customers. Customers want to log in; they want to initiate transactions, even create new accounts with a really user-friendly experience.

But on the other hand, fraud is here to stay, and it seems like with every new functionality you introduce, there's the opportunity for fraud. So these financial institutions are really facing a constant attack, and they can't ever let their guard down when it comes to security. They've built their whole reputation around trust.

So with all these new digital innovations they have to build out, they also have to give security just as much thought. And that leaves some real tension.

How do you balance that great customer experience without compromising on security, authentication and trust? Confident security powers confident innovation, so institutions that really want to ride that wave of the digital transition have to deliver the right security in the right place at the right time to create experiences that are both secure and customer-centric.

Customer Retention

FIELD: Well, Valerie, that's a great way to set this up, and given your description of this tension, let me ask you about risk in terms of two areas: first, talk to me about risk in terms of customer retention.

BRADFORD: Customers today are really eager to engage with their bank over the digital channel. At this point, it's pretty clear that modern consumers are really expecting to be able to interact through their computers, their tablets and their mobile devices any time and anywhere. And if the digital sales process is too complex,

if there are too many steps and authentication challenges, users often abandon the activity, and that can mean lost business.

So if you can't provide that digital experience in a secure and seamless way, you're at risk of falling behind. You might see that in reduced brand loyalty, fewer new customer acquisitions, lagging net promoter scores and even high rates of abandonment on the new account creation process. And every day, there are new startups coming into the financial industry, and they may become a layer between the bank and the user. So banks should be really feeling that pressure to deliver the digital experience, because there are others who will happily step in, and the banks are going to find themselves just as a transaction platform or a commodity.

New Forms of Fraud

FIELD: So there's that frictionless customer experience we talk about. If you don't provide that, you're going to lose your customers. But you then risk opening up your customers to new forms of fraud. Talk to me about that.

BRADFORD: It should go without saying that no matter how exciting or customer-centric you can make the user experience, you have to have complete security. Protecting your customers' money and identity is just table stakes. But with today's threat landscape that's really hard.

With all the data breaches of the past few years and the explosion of information-sharing happening on the internet or social media, old ways of securing and authenticating accounts using personal information are starting to feel a little bit useless. The Equifax breach alone compromised personal information for more than 145 million people.

So bad actors are out there. They're able to use these real identities stolen from breaches to open new accounts or take over existing ones, and that's really hard to detect. The threats are constantly evolving. You have to keep up with all kinds of financial fraud, malware, social engineering, phishing emails, remote-access Trojans. So the threat landscape is in constant flux.

What's at risk in terms of fraud is, of course, your monetary loss. But it's a lot more than just that stolen money; it's also the time and the effort that you spend working with your affected customers, the remediation costs and all of the operations costs that come with the fraud and the fraud detection. And your reputation as a secure financial institution is on the line.

Challenges in Banking

FIELD: So, Valerie, you've got an advantage at IBM Trusteer, where you get the opportunity to see lots of organizations in lots of different sectors. Where do you see banking institutions in particular falling short in trying to address this challenge between fraud and customer satisfaction?

BRADFORD: As the banks are activating these new channels, they are aware of the security challenges, and they're reacting by focusing on stopping fraud. That brings up two big areas where they fall short.

"If you can't provide that digital experience in a secure and seamless way, you're at risk of falling behind."

First, they're doing all these things to stop fraud, and they're probably also stopping real customers by making it harder to open an account or to log in or complete a transaction. Customers are likely leaving to find an institution that can provide them that digital experience.

But the second place where we see banks falling short is when they're building all this new fraud protection, but they're not really stopping fraud. We see a lot of institutions out there that are implementing what we think of as one-trick pony solutions. These are solutions that claim to offer complete fraud protection, but in essence are just device ID, or just behavioral, or anything like that. And all of these tools are good: they're important to have in your toolbox. But if that's all you have, you've got some real vulnerabilities. So criminals can navigate around any single layer of security.

For example, bad guys are getting around device ID by using remote-access Trojans, so they can take over a user's actual device and use that to interact with the financial institution. And that's going to be hard to catch if you're relying too heavily on just device

> "We see a lot of institutions out there that are implementing what we think of as one-trick pony solutions."

ID as a fraud protection. That's why we really want to see more and more banks thinking about multilayered security strategies.

IBM Trusteer's Role

FIELD: Well, Valerie, toward that end, talk to me about IBM Trusteer. What are you doing to help organizations to be able to transparently assess new digital identities?

BRADFORD: IBM Trusteer helps detect sophisticated criminal activity right from the start of your interaction with a customer, from assessing risk levels of a new customer, to login process to monitoring transactions. It offers multiple layers of machine-learning technology combined with intelligence and security services. That's behavioral/biometrics, malware detection, device ID, transaction monitoring and more, just to help build digital identities and allow financial institutions to better differentiate between legitimate customers and criminals.

IBM Trusteer analyzes billions of activities every day ... with a worldwide fraudster consortium. And this helps banks by leveraging the digital channel to generate growth and build transparent security for digital customer experiences that are both more secure and more seamless. ■

Listen to the interview online: https://www.databreachtoday.com/interviews/banking-in-balance-security-vs-convenience-i-3878

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.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY

ISMG
INFORMATION SECURITY
MEDIA GROUP

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