FDIC
PODCAST
SPECIAL SERIES
Banking on Innovation

Episode 6 – Verifying Identity in a Digital World

SULTAN MEGHJI: Welcome to the FDIC Podcast: *Banking on Innovation*. My name is Sultan Meghji, Chief Innovation Officer here at the FDIC. While it might be true that cash is king, we're increasingly living in a world where nearly every aspect of our financial lives is done digitally. We shop, we bank, buy, sell, pay, whatever on our mobile devices or computers.

And at the center of all of this activity is digital identity. After all, proving who you say you are, is foundational to enable our digital economy to function. The tech lab I lead here at FDIC, we call it FDITECH, is teaming up with the Treasury Department's Financial Crimes Enforcement Network, called FinCEN, on a tech sprint to come up with an innovative new way to measure confidence in digital identity proofing. That's the process you use to collect, validate, and verify information about a person.

Joining me to talk about this sprint is Justin Cole, he's a presidential innovation fellow here at FDIC and the resident expert on our tech sprint program, as well as Kay Turner, senior counselor to the director of FinCEN, welcome to you both.

JUSTIN COLE: Good to be here.

KAY TURNER: Thanks so much.

SULTAN MEGHJI: I am incredibly excited for this conversation…first off, because for those who've been listening to these Banking on Innovation Podcasts, Justin has been kind of the Machiavelli in the background, the guy actually doing all the work, it's absolutely fantastic. And Kay is one of my new best friends in the federal government since I joined. Just one of the coolest people. So I'm so excited to have both of them here with me today.

Let's dig into two things cause really we're here to talk about this new tech sprint that FDIC and FinCEN are working together on. But maybe it'd be useful for the audience, Justin I'll turn this over to you, let's give a primer, if you will, on what a tech sprint is here at FDIC and what we're doing there.

JUSTIN COLE: Yeah, absolutely. So, tech sprints are really just short, intense problem-solving sessions that bring a diverse group of people together to untangle a complex problem, rapidly develop a prototype, and then test that prototype to actually see if it works.

The tech sprint culminates in a demonstration day, so think of this as kind of a pitch session where each team has less than 10 minutes to really kind of share their idea to a group of judges who evaluates each team and presents awards to the top ones.

Tech sprints have been used by quite a few federal regulators, both here in the U.S. and internationally. The first probably was from the Financial Conduct Authority (UK) in April of 2016. So to think that we as regulators have been doing this for only the last five years is pretty amazing. When you think about all of the different topics that we've covered in that timeframe from, you know, certainly here at the FDIC, looking at topics of financial inclusion and operational resilience. The Consumer Financial Protection Bureau has used tech sprints in order to look at things like housing insecurity. And needless to say, if the problem is sufficient in scale, and likely to motivate a large number of people to participate, it's a good fit for a tech sprint.

And so, you know, we're really excited. We've seen a number of impacts, success stories, coming out of the two tech sprints that we've hosted to date. We've had over 750 attendees attend one of our first two tech sprint demo days. We've seen new solutions developed that are actually having an impact in the market today. And then we've also seen a lot of conversation, energy, panels that have resulted from some of these tech sprints. And so, you know, if you're out there listening and you know, these kinds of topics interest you, if you're motivated to solve societal challenges, develop your network, strengthen your pitch skills, I hope you'll consider applying for our next tech sprint, uh, which I'm so excited to, uh, be able to talk with you all about today.

SULTAN MEGHJI: Well, let's jump right in. If somebody wants to participate, what do they do Justin?

JUSTIN COLE: So, be sure to check out fdic.gov/FDITECH and right on that webpage, you should see a registration link, uh, provide a few details about your participation. And we are very excited this for this first…this tech sprint will be the first time we'll have actually individuals register. So, you know you can be affiliated with an institution or completely unaffiliated and just somebody who wants to contribute to this work. You go on there, register online and, you know, we'll be reviewing registrations and selecting registrants within a couple of weeks and let you know the next steps after that point.

SULTAN MEGHJI: So Kay, you know, I'm not sure everybody who's listening really knows what FinCEN is. Could you spend just 30 seconds telling us what FinCEN is?

KAY TURNER: Certainly I'd love to provide you a bit of context about why we were so delighted to work with the FDIC on this important subject. Before I do so, I just wanted to thank the FDIC, Sultan, Justin and the rest of the team for this opportunity for both me and the FinCEN digital identity team to work on this digital identity tech sprint. We're really hoping to advance our understanding of how digital identity can help safeguard the financial system.

So a bit of context: FinCEN's job is to safeguard the U.S. financial system as a primary administrator of the Bank Secrecy Act and the U.S. Financial Intelligence Unit. We focus on illicit use, money laundering and related crimes, including terrorism and help to protect us national security. We work with over 150 international partners and thousands of domestic regulatory and law enforcement stakeholders to identify and investigate illicit actors exploiting the financial system.

So identity sits at the heart of that role, the ability to detect and address risk is only as good as the ability to determine with whom you're engaging. To get financial services right, we got to get identity right. And to do so in a way that preserves privacy and security while ensuring integrity in the financial system.

In fact, last year, weaknesses in our current identity and payment systems were highlighted when we saw billions of dollars of COVID relief-related program fraud. These considerations have motivated us to better understand how identity is managed, verified and authenticated. Because at the end of the day, identity is a network business. So it's really important that we bring public and private sector minds together. We got to collaborate on the future of identity and related innovation.

SULTAN MEGHJI: Let me make this meaningful for the listeners. I want you, Kay, to describe your goals, or FinCEN goals I should say, in this collaboration and what you're hoping to get out of this tech sprint.

KAY TURNER: So I think, you know, when I was talking about this collaboration, it's going to take the intellectual power and creativity of all of us to figure out how to secure identities and prevent illicit actors from exploiting identity and financial crime. This is, you know, protecting the U.S. national security and supporting law enforcement. So we view this tech sprint as a great way for FinCEN to learn about ways to assess the efficiency and effectiveness of customer identity…a fundamental component of protecting the financial system…by convening, bringing in, and working directly with many of society's different perspectives to throw, to solve this shared problem. You know, we'll be bringing together people from industry, academia, subject matter experts, government leaders, civil society, and regulators in the same room. This is a unique opportunity. And when we think about it, we expect when we're working together on the same team and bringing all these perspectives, we're going to, we're going to provide substantial dividends and it promises to be a force multiplier for creative problem solving for one of the most challenging problems for the financial sector.

SULTAN MEGHJI: You know Kay, hearing all of that, it's really interesting to me to consider that we talk about risks and we talk about problems, but like, what are we actually gonna be able to solve if we get digital identity right?

KAY TURNER: What we're seeing is an evolving set of threats. We're seeing identity exploitation and financial crime. We're seeing issues at the account opening stage, when financial institutions need to collect, validate, and verify customers' documents, otherwise known as proofing and verification. We're also seeing the manipulation of digital images to undermine KYC (Know Your Customer) checks. You know, we're seeing issues with unauthorized third parties getting access to accounts, and what's called account takeovers with billions of compromised credentials exposed online, there's a high likelihood that Sultan, some of *your* legacy information has been compromised!

Criminals are using exposed names and passwords to log in to other people's accounts. Otherwise known as credential "stuffing attacks." These compromised credentials create more opportunities for ransomware implementation on business networks. FinCEN is receiving reports of more sophisticated methods of account takeovers. I mean, since I joined FinCEN in June, I've learned about compromised authentication applications, SIM swapping, single sign-on and account aggregator services exploitations. However, compromised passwords and security questions in single-factor authentication exploits still account for the vast majority of account takeovers in suspicious activity reports filings. So the bottom line is that many account takeovers and fraud are occurring because of insufficiently strong identity verification and authentication.

SULTAN MEGHJI: Justin, can you, you know, one of the interesting things we had to do is we thought through this tech sprint is keeping two slightly different sets of interests at play, right? FDIC has one interest in one set of statutory authorities, FinCEN has another…can you spend a few minutes just talking about, you know, kind of the process you went through over the last few months to help put this together?

JUSTIN COLE: Yeah, absolutely. So I think, you know, we started this tech sprint as we do with every tech sprint of really looking at, you know, the scale of the problem. How, how big of an issue is the particular area that we're starting to look into. We also sought to ask the question of who are the stakeholders, right? Who are the groups, who are the people out there doing work in this area? And can we find kind of a convergence of scale, application to our kind of regulatory mission, and just public interest of folks who are going to be interested in applying and participating.

We then had the, I think, really welcome opportunity to think about, uh, adding another layer on top of that, of how do we, FDIC and FinCEN, find that intersection point, that point at which, you know, both agencies, you know really, have areas that we, you know that we can dig into.

And so, you know, I think we really started with, as we do with everything, a bit of research and discovery…understanding what are some of the emerging topics and issues in this area. We met with a number of stakeholders across the FDIC to think about, you know, this issue from, um, from both an operational risk point of view, as well as from sort of a technology point of view. And I'd like to think we've found kind of that sweet spot that, that problem statement, that topic area that not only will attract, I hope a great deal of attention and a great deal of potential participants, but will also help to focus squarely on the topic of digital identity and how do we think about that going forward, which I know again is a, is a topic of interest to both the FDIC and FinCEN. So again, was really exciting kind of creative process and, yeah, we hope that we've set it up in such a way that, that really the participants will take it and, and come up with some really great ideas.

SULTAN MEGHJI: Kay I mean, you guys have obviously seen a lot of, a lot of digital identity change in the especially last 24 months around COVID, you know, is there anything that's kind of top of mind for you that that's, that's worth talking about?

KAY TURNER: I think I had highlighted this whole issue of COVID relief program. And we certainly saw a big uptick and the number of Suspicious Activity Reports (SARs) between February 2020 and June 2021. We had over 330,000 of those submitted by financial institutions and industries referencing COVID. You know, government program-related SARs accounted for nearly six percent of the almost five million SARs filed. You know, it's really unusual to have such a large amount of SARs filing connected with a single issue. And in this case, its potential COVID-19 related. We saw upticks in account takeovers, you know, compromised usernames and passwords that were used rose by 12 percent or around $6 billion. Cyber event SARs where stolen data that drive future identity compromises expanded by around three billion to eight billion. These are large numbers. And so one of the things is that FinCEN had been looking at digital identity and brought me in to lead the agency. And it's really been a wonderful experience working with my colleagues to figure out what we can do about it.

SULTAN MEGHJI: You know, it's really interesting. And I love hearing this drum beat from across the U S government. We say it, you say it, you know, Chris Inglis, the National Cyber Security Director has said it…that it's all of us together. It's not just the public sector, it's not just the private sector, it's not just academia…it's all of us working together for the betterment of our country. I'm just blown away that we got this sorted out and we can do actually do this tech sprint together. I think it's awesome. It's a new territory for all of us but I can't wait to see what comes.

So thank you both so much for joining us here on the FDIC Podcast. Thank you. Kay. Thank you, Justin.