SentiLink

# Navigating Regulated KYC Webinar

## TRANSCRIPT

**November 17, 2021**

**Moderator:** Naftali Harris, Co-Founder, CEO SentiLink
**Panelist**: George Seeberger, General Counsel of 1st Financial Bank USA
**Panelist**: Robert Rowe: VP, Sr. Counsel with American Bankers Association
**Panelist:** Parag Patel: Senior Associate with Orrick,

**Naftali:** Thanks so much for joining our webinar on first principles in KYC. I'm Naftali Harris, the Co-Founder and CEO of SentiLink. SentiLink stops fraud and now does KYC for over 100 financial institutions in the U.S. We're delighted to have you here to talk about KYC. We think there's a lot of fear, uncertainty and doubt around KYC, CIP, Red Flag Rules. We took a very first principles approach on how to comply with CIP. So, we've put together a panel of experts to talk through what the rules mean, and their history. I'm the only non-lawyer here and I do want to say anything discussed here is not legal advice.

Let's start with introductions.

**Parag Patel:** I'm a Sr. Associate at Orrick Herrington & Sutcliffe. My focus is largely financial services regulation and fintech

**Rob Rowe:** I'm VP, Sr. Counsel with ABA. I've been with ABA for 15 years and I've been doing BSA/AML for 30 years now. I've been fortunate to have been a member of the Bank Secrecy Act Advisor Group for nearly 25 years. I was there when CIP rules were first drafted.

**George Seeberger:** I'm General Counsel of 1st Financial Bank USA. Prior to this role, I practiced law at Winston and Strawn and was an Attorney at the Federal Reserve Bank of NY.

**Naftali:** Parag, can you give us an overview of the CIP rules?

**Parag:** CIP stands for customer identification program. CIP is a rule that says banks have to have a program with risk based procedures to verify the identity of a customer to the extent it's reasonable and practicable. The terms reasonable and practicable are really important because it's not an absolute. There's a standard of reasonable-ness here. The procedures should enable the bank to identify the customer's true identity, and they should be based on the relevant risks to the bank. It takes into account the customer base, the type of account, the location. All the types of factors that influence risk.

From there, CIP requires collecting 4 pieces of data on each customer. Name, SSN, date of birth and address. If you're an entity, then the beneficial owners are required to give this data.

Credit cards are a little different, where the data doesn't need to come from the customer. It can come from bureaus, for instance.

Once you have this information, what do you do with it? You have to verify the identity of the individual within a reasonable amount of time after the account is opened. How do you verify the identity? You can do a documentary verification, non-documentary verification or a combination of both. Documentary verification could involve looking at a drivers license, for example. Non-documentary verification could entail pulling a credit report, using Clear, LexisNexis, or any 3rd party vendors that access public databases. You take the data from the applicant and try to match with the data from these vendors. There may be additional verification requirements in certain areas.

What happens if you aren't able to verify? You also need a procedure around that. It has to include what account should not be opened, and when you should file a SAR if you are a bank.

There are a couple final elements of the rule around recordkeeping, and the boilerplate disclosures that have to be communicated to applicants when you collect information. Then there's reliance on other financial institutions. You don't see this as much in the fintech space.

**Naftali:** Rob, can you tell us a little about the history of CIP?

**Rob:** In the early 1990's, there were a large number of NY banks that were looking for guidance on what they were supposed to do in terms of verifying their customers. The Federal Reserve put out a Know Your Customer guidance. For a variety of reasons, it backfired badly, and there was a lot of resistance particularly from privacy areas. The Fed got a lot of comment letters opposing it. They were criticized by Congress. But the idea was around back then that we didn't have a formal mechanism to identify who our customers were.

Then we had 9/11 and the Patriot Act which was essentially a potpourri of things that hadn't been able to get through Congress in the last 20 years. But, one of the things that was included was the Customer Identification Program Rule. It required the basics that Parag that went through which is important, but when the rule itself was being developed, conversations were really centered around what banks were doing now. What kind of steps were they taking? What they were looking at for a customer that was coming into a branch. This was 2001 and 2002. There were very few digital accounts. A lot of banks at that time required people to physically come into a branch to open a new account and present their drivers license. What came out of that was the belief that the only way to verify someone's identity was with a driver's license if they are from the U.S. and a passport if they are from overseas. A lot of banks forgot about the non-documentary and other ways you can verify someone.

What we're seeing now, especially with the pandemic, is we've moved to virtual and we are moving to digitization so everyone's looking at whether there are digital ways to do this.

We're considering whether we still need to have the same CIP procedures as we move online. Do we really need to collect the name, DOB, SSN and address? Are there other ways to verify identity? We're getting to a tipping point where we're going to see some changes.

**Naftali:** George can you give an explanation of how to comply with CIP?

**George:** CIP compliance procedures vary by type of financial product and how it's sold. CIP procedures for new bank customers may differ for people walking into a branch from those applying via digital channels or mobile app. There are some commonalities to the policies.

My example of CIP procedures is for someone who is not an existing customer and who is applying for a credit card. For all new accounts, what we'll look at and what we'll collect is what we call, "identifying information." That identifying information is going to include name, DOB, SSN, address. For a business, we'll look at EIN. For non-U.S. citizens, we'll look at taxpayer identification, passport number and country of issuance, we'll look at alien ID numbers or similar picture ID's. For a non-US entity, we'll try to get a government issued document certifying the existence of the business enterprise.

For an individual, we compare the identifying information with information we've obtained about that applicant from a credit bureau, public database, or other trusted third party source. If the identity matches, this part of CIP is completed. If no information exists, then we'll contact the person to confirm he/she requested the credit card, and request documents verifying the identifying information. We require a copy of an unexpired drivers license, military id card or state issued id card, passport, US alien registration card, or some other similar government issued id that contains a picture of the applicant.

If we're unable to identify the identity of a person, then we will not open the account for that person. Except when there are reasonable extenuating circumstances. In those circumstances, the account may still be opened so long as the discrepancies in validating the identifying information are resolved in no more than 60 days after the account is opened. If the identity can't be verified in that amount of time, we will close the account. And if credit has been extended to that account during that time, then we will send an adverse action notice to the account holder.

That's what our policy is and how we identify someone for CIP purposes.

I also have a quirky example to share of how we went through CIP in a very recent example. Our bank got 2 credit card applications around the same time with 2 different names, date of births and SSNs, but the same address. On one app, the address didn't match the address on the bureau. On the other app, the SSN didn't match the SSN at the bureau. As such, the bank was unable to verify the identifying info in each application. So, the bank contacted the applicants to get a copy of an electric bill. The addresses on the bill matched the address on the bureau. And, the bank also asked for passports to verify each applicant's identity. The passports were issued by two different offices, but the picture on the passports was the same. So, we had

two different passports, two different names, but the pictures were the same. So the applications were declined. The decline reason was that the bank was unable to verify each applicant's identity. In this case it was likely that both applications contained some sort of synthetic fraud.

Before opening any new account, we compare the name of a prospective new customer to the names on the OFAC list. An account won't be opened for anyone whose name is on an OFAC list.

It's proper to have BSA/AML and customer due diligence programs based on the type of product. So, even if the customer gets the product they applied for, credit card or prepaid card, for example, there are programs that put restrictions on certain transactions that involve a particular product.

**Parag:** Just want to piggyback on what George was saying on OFAC screening. This is something I see a lot with clients that are domestic that have no international customers. It's a check the box exercise for them. But I like to remind them that there are a number of people on these sanctions lists that reside in the U.S. The probability is it may not be your customer, but there are companies in the U.S. with exclusively domestic products that still need to think about OFAC sanctions. It's an absolute liability.

**Naftali:** What's interesting about George's example is the amount of care that goes into figuring out if the people that are applying are who they say they are. To the point of noticing something that was off on the utility bill and then finding 2 different passports with the same picture, it's clear a lot of effort goes into this. Parag you mentioned the reasonable belief needed to determine the true identity of the applicant, there's a lot of information packed in that short sentence.

**Naftali:** What is the biggest misconception to KYC?

**Rob:** KYC is done at account opening and you're finished with it. George mentioned you have different levels of KYC depending on the products and services that are being used. A friend of mine at the FDIC would say the amount of diligence on a plain vanilla account is lower, but it's an ongoing process. Particularly if you think about sanctions. Someone who's not on the sanctions list today could be on it six months from now. So you have to have a process that keeps updating your customer information.

**George:** It may be a misconception to think of CIP as a check the box exercise at the beginning of an account relationship. Obviously you have to do it. If you don't do it, it's a compliance violation. It's seen as a "gotcha" exercise if you fail to do it properly. But it can be more than that. In the examples I gave, we prevented a couple cases of fraud. CIP can be used in a way to improve fraud detection and make your business better. You really do understand your customer a little bit more, and where they're coming from and it can be used as a positive especially on the fraud side.

**Parag:** In my prior life I used to be in-house counsel at Capital One. And, we thought of fraud and AML as hand in hand, both in the org chart as well as in the processes. As George pointed out, a good CIP program can help mitigate fraud risk. I know there's a lot of clients taking that same approach of leveraging fraud services in the CIP space and vice versa.

**Naftali:** I'll take that a step further. There's a lot of belief that there's compliance and there's fraud, and in many cases never the two shall meet. If you read the CIP rules,it states you must have "reasonable belief" of the true identity of the customer - - were you not doing that already in your fraud program? Over time we'll see that these two functions are a lot closer than you might think.

**Parag:** I think that's right Naftali. For AML, one of the key pieces is layering. If you need to layer funds into the system, what's the best way to do that? Fraudsters. They fraudulently make a synthetic identity and layer the money into the system. I do think they go hand in hand.

I'll also throw out my misconception here. There are two things I'm noticing quite a bit more with fintechs and neo banks. One is who has the legal obligation to do the BSA/CIP? The second is around international. As a matter of law, the Bank Secrecy Act pertains to financial institutions. There are 27 entities defined as financial institutions under the rule. Fintechs are generally not financial institutions. Some of them are like ones that have MSB licenses. Fintechs have to comply with BSA/CIP rules specifically because of contracts. It's important when you think about your sponsor bank relationship because they should allocate responsibility to these things that don't apply to the tech company on its face, but apply through contractual provisions. And there are certain provisions that will never be able to be applied to fintechs. Things like CCRs (Comprehensive Credit Reports) and SARs (Suspicious Activity Reports). Fintechs don't have access to file a SAR. That's exclusively done by the FI, same as CCRs.
That's important to think through as you're breaking down obligations as well as how information should flow.

The 2nd thing is around international. How you facilitate cross border money movement. How you bank people not from the U.S. What I'm seeing is conventional financial institutions that are sponsoring fintechs always have a little bit of heartburn around international customers. They will say it's because of BSA/AML. But that's a red herring here. The CIP actually contemplates international customers. It says, if you're an international customer, without an SSN or TIN, here are other things you can use like a passport, Inherent in that is that you can bank international people. There are other issues of banking international people that relate to the jurisdiction - like if you are banking someone in France, does a French regulator care that you're offering bank services in their country. That's a totally different question. But, I always hear people blame BSA.

**Naftali:** Interesting stuff. What are other hot topics related to KYC.

**Rob:** One of the things that's not really that surprising is the idea of beneficial ownership and it's still a discussion topic internationally. The Financial Action Task Force is still looking for ways to

improve collection and verification of beneficial owners. In the U.S., we're waiting for FinCEN's development of a beneficial ownership registry. We're waiting for guidance any day now on rule making on who has to report and who will be covered by that regime. The availability of that information, what it's going to mean for FI's, is going to be important. Once they determine who's going to report, having that wealth of data is going to be a game changer for Know Your Customer.

**Parag:** AML Act of 2020 came out last year. And FinCEN's supposed to have rules out in Jan 2022 which seems unlikely to happen. They haven't even given us proposed rules. It's just notice of rule making right now. Also, cryptocurrencies and NFTs are interesting in the KYC space because there's a high risk for money laundering but how does that interact with the AML Act of 2020? We've understood for the last 5 years that cryptocurrency itself is regulated under MSB activity. FinCEN put out a bunch of letters on this in 2019, they synthesized and put out one long piece about how they think about exchanges, administrators, issuers. They talked about all these elements of the cryptocurrency environment. Congress adds that to law and says anything that has a value that substitutes for currency is regulated but nothing really changed there.

What's more interesting is the inclusion of antiquity dealers as financial institutions as outlined in the AML Act of 2020. There were a lot of studies that came out saying there's a lot of money laundering that happens at antiquities dealers where many anonymous 3rd parties buy an old Van Gogh and millions of dollars gets layered into the system and no one knows who these people are. So, Congress said this is a problem and told FinCEN to go regulate these antiquities dealers as a financial institution. But, what's an antiquities dealer? What's an antiquity? An old greek statue? It's unique. Only one person can own it. An NFT has some of the same characteristics of art or antiquities. It's unique. There's only one of them out there. Does that count? The next layer of all of this is that FinCEN is supposed to produce a study on whether art dealers should be regulated financial institutions. What if you're an issuer of NFTs or seller of NFT, are you an art dealer? These are some of the interesting stuff happening that's based around crypto (we kind of get a little more guidance from FinCEN for AML purposes). But, it doesn't address all this new stuff that's coming out in crypto like non-fungible tokens (NFTs).

**George:** There's development going on with beneficial owner rules. Most banks won't do business with a company engaged in cannabis. But, what if you're getting requests for bank products from the owner of a cannabis business? Where are the funds coming from that the owner is looking to deposit or what's the source of repayment if they need a loan? Most banks are reluctant to touch that customer due to federal laws around marijuana. This is one situation where revisions to beneficial owner rules may affect that situation or make it clearer.

Something else that's interesting is using block chain to reduce id theft and make CIP easier and less costly to complete. By this I mean how to use blockchain to take card forms of identification and combine in a blockchain id. Instead of showing the doc or using a credit report to match to, the consumer produces what's known as a secure and immutable public key that's generated by a blockchain ledger. This could allow consumers to verify identities without having

to share personal data and also from the bank's point of view, it simplifies the authentication and makes it more secure.

What's also noteworthy is the use and growth of eCBSV. That has to do with Social Security numbers. In June 2020, the Social Security Administration launched its **E**lectronic **C**onsent **B**ased **S**ocial Security Number **V**erification service. It's another way of trying to use an electronic database to identify customers and reduce the incidence of synthetic identity fraud.

**Naftali:** We were the very first company to go live with it.

**George:** Oh really, that's interesting. I did not know that. That's impressive.

**Naftali:** Additional fun fact, I, Naftali Harris, was the very first consumer to go through it. And, Jason Kratovil is also now with SentiLink. He's the guy that got Congress to pass the law calling for eCBSV. He now runs government affairs for us.

As for eCBSV, the industry was excited from the perspective of stopping synthetic fraud. One thing underappreciated about it is how helpful it can be for KYC especially for certain segments of the population like immigrants, young people, new to credit who don't have any previous history. The first time they apply for a financial product, they get rejected because there's no evidence they're a real person, they have no history of credit. They end up failing KYC. Now that the SSA has this program, eCBSV is going to be a meaningful part of KYC programs going forward.

**Natfali:** What do you think the future of KYC looks like?

**Rob**: Development of digital identity. Both the Department of Treasury and Federal Trade Commission have projects that are analyzing all different aspects of digital identities. How you do it is a question. Should it be the private sector, should banks be the ones issuing digital identities. How do you coordinate them with other financial institutions? Or should it be the government? We're used to the government issuing passports and social security numbers. Are they the appropriate repository for the issuance of digital identities. But, the ability to use digital identities goes back to what I said earlier as more things go online the ability to use a digital identity certainly facilitates things. There's two sides to it. One is CIP, the basic information you need to open an account. But over time through the relationship that an FI has with a customer, you develop a more comprehensive set of information about them. How they behave. How they use their accounts. What kind of transactions they use. You develop a more thorough way to verify their identity. This will be exciting in the next couple of years.

**Parag:** There's a trend for digital identity but it's also an issue with privacy. India has something called the Aadhaar System that has given a digital identity to 1.3B people. The U.S. thought about doing that in the 1970s, but it got a lot of pushback because of privacy. The same idea is now reappearing. We'd love digital identities to streamline things like medical care and financial services, but it goes against privacy. There's also another wrinkle here. State level privacy. If

you think about Illinois, for example, it has one of the strongest biometric statues out there. If you use any service that captures your image, and you scan your id, those vendors require a lot in terms of consent because of places like Illinois. CA is similar with CCPA, but I think Illinois is way thornier for biometric statues. A lot of states exclude data that falls under GLBA which includes AML covered data. What happens when states drop that stuff out? It impacts FI in a big way. This is what came up during the lobbying for CCPA. What the banks really pushed for was something similar to GLBA which was an entity level exemption to use data the way we need to use it - so banks could develop digital identities. CA said, “no, we’re not going to give it to you based on entity type, we’ll give it to you based on data type.” From a data protection standpoint, that makes a lot more sense, but it makes it harder to make digital identities unless they’re done by banks in connection with a financial product. This all relates to how privacy interacts with AML.

**George**: I agree with the use in digital identities. Banks using web cameras to identify customers. The other thing to point out is not to be so U.S. centric focused and where developments are coming. There’s also rules going on in Europe - they may be ahead of us. The AML 5 and EIDES procedures are two examples. They pertain to the use of digital tools in terms of trying to do CIP.

**Question from the audience:** Are there any more things like eCBSV on the horizon?

**Naftali:** I know of at least 2 on the horizon. One is for 4506T that the IRS offers to get copies of consumer tax returns. The IRS is working on automating that. There may be something similar for beneficial owners for FinCEN where they are working to put a database together.

**Rob**: There are a couple utilities out there. One is SWIFT, the international messaging service. The other is the Depository Trust Company of NY. I’m not sure what is the status now, but if a commercial customer says “yes I give permission for XYZ bank to access my data,” instead of having to provide the beneficial ownership information, each one of the FI’s that you have an account with you just pings this one major database to get the information and they would keep it up to date. Some of those are on hold as FinCEN develops its registry. The 64,000 question is how much access financial institutions will have to what is in the FinCEN database.

There is a lot of effort by the private sector to develop some of these utilities to make it easier to do KYC and customer identification.

**Naftali:** Parag you mentioned the system in India, there are plenty of other countries that have systems like this. Singapore has Identity API, Estonia has public key cryptography that they embed in their ID’s. I think the US would be better off if we were to have such a system. I don’t think we’re going to see the Federal government step in and do that for the privacy sort of concerns mentioned. I believe the private sector will step in and frankly that’s what we’re trying to do here at SentiLink.

**Rob:** We're seeing a lot of concerns about privacy. The companion piece to that is data security. Whenever a federal agency wants to collect more data, we remind them of the importance of making sure what they collect is maintained in a secure way.

**Naftali:** We certainly have our work cut out for us. Thanks all for participating!