EPISODE 8 | Webinar Recap & Discussion

Fraud & AML Executive Insights for 2026

MARCH 2, 2026

This transcript was auto-generated and may contain errors or inaccuracies.

Jeff Welcome to "What the F Happened? Fraud and Financial Crime Deconstructed," a DEFEND podcast where we break down what's actually happening across fraud, scams, AML, and financial crime.

Emily Each episode cuts through the noise to explain the tactics, trends and real world impact behind the headlines so you're better prepared for what comes next. Let's get into it.

Jeff So imagine a race. But it, uh, it isn't exactly a fair one, right? In fact, it's completely lopsided. On one side, you have the banks, you know, these massive financial institutions holding everyone's money. Yeah, they're running this race, but they're wearing heavy ankle weights. We're talking regulations, privacy laws, internal bureaucracy, legacy software.

Emily That's probably older than you are.

Jeff Exactly. Yeah. And then, uh, on the other side.

Emily You have the fraudsters.

Jeff Right? And they are just running. They are sprinting. And to make matters worse, someone just handed them a jet pack.

Emily A jet pack called artificial intelligence. Yeah, it sounds super dramatic. Kind of like the opening of a techno thriller. But that is exactly the landscape we're looking at today. It's this digital arms race where the offensive weaponry is evolving. I mean, significantly faster than the defense systems can keep up.

Jeff And that is exactly what we are digging into for today's deep dive. We've got a really serious stack of papers here. We're looking at a high level executive report and a technical webinar.

Emily It's titled “Executive Report Insights.”

Jeff Right in the lineup on this panel was just heavy. We're talking Yinglian Xie, the CEO of DataVisor, Brian Hughes, from Affirm, David Barnhardt from Datos Insights, and Ted Josephson from Synchrony.

Emily Yeah, these are the heavy hitters. You have the technology providers, the strategic advisors and the people actually fighting the fraud in the trenches.

Jeff Like people doing the actual work.

Emily Exactly. And their mission here was to look ahead, specifically targeting 2026 and 2027 and figure out what the future of anti-money laundering or AML and fraud prevention actually looks like.

Jeff So let's unpack this for you all listening, because the very first thing that jumped out at me from their discussion was this concept of the AI paradox, which sounds like a scifi trope, but for a bank, it's a massive operational headache. What exactly is the paradox here?

Emily It's the core tension of the whole industry right now. The paradox is that the attackers are leveraging AI to move fast, break things, and really scale up their attacks. Meanwhile, the defender the banks are stuck moving deliberately, right? They can't just unleash AI because they have to worry about model risk management, regulatory fears, and of course, data privacy.

Jeff Let's actually pause on moderate risk management for a second. For the uninitiated, that sounds like, I don't know, corporate speak for just being careful.

Emily It's a lot more than just being careful. Think about it this way if a hacker uses AI to write a phishing email and the AI makes a grammar mistake.

Jeff Who cares.

Emily Right? Who cares? The hacker just tries. Again, it's totally low stakes. But if a bank uses AI to flag a transaction as illegal and, say, denies your mortgage payment or locks your account by mistake, that is a regulatory nightmare. Banks have to prove, both mathematically and legally, that their AI models can explain exactly why they made a specific decision, right?

Jeff A hacker doesn't have to fill out a compliance form or explain to an auditor why they launched a phishing campaign.

Emily Exactly. And the numbers really back up this anxiety. In the report, seventy four percent of risk leaders identified AI driven attacks as their top threat.

Jeff Wow. 74 percent.

Emily It's a staggering majority. They know it's coming. Or rather, they know it's already here.

Jeff But here's where it gets really interesting to me. I sort of assumed AI fraud meant we were going to see brand new, never before seen types of super crimes.

Emily Like Ocean's eleven, but with robots.

Jeff Yeah, exactly. But Ted Josephson, he kind of pumped the brakes on that idea. He said it's not necessarily new fraud.

Emily That's a crucial distinction to make. Ted called it the scale and sophistication of the same old, same old.

Jeff Same old, same old.

Emily Yeah. The bad guys are still trying to do the classic things take over your account, steal your identity, trick you into sending money. But AI allows them to do it with a level of polish and a sheer volume that was physically impossible for humans to do alone.

Jeff The Polish part is what really scares me. Brian Hughes mentioned that the days of spotting a phishing site because of a typo or a pixelated logo. Those days are over.

Emily Completely gone. AI can now create bank lookalike websites that are pixel perfect.

Jeff Unbelievable.

Emily I mean, identical code structure, identical visuals, and it goes way beyond just websites. They're using AI to bypass document verification. You know those static selfies you have to take to prove you are who you say you are for a crypto app or a neobank.

Jeff Oh yeah, where you have to hold up your driver's license to your webcam and look super awkward. I always feel ridiculous doing those.

Emily That's the one. AI can now generate falsified credentials. So fake driver's licenses with your name on them, and fake video feeds that look real enough to actually fool those verification systems.

Jeff So the whole concept of trusting your eyes is basically dead in the digital space?

Emily Pretty much. But perhaps the most disturbing part, which David Barnhardt pointed out, isn't the technology itself, it's the economics. He calls it the democratization of fraud.

Jeff Democratization. That phrase really stuck with me. Usually that sounds like a good thing. Power to the people. But in this context, definitely not.

Emily No, not at all. He's talking about the blue collar fraudster. In the past, to run a sophisticated international scam, you needed money, you needed deep technical coding skills, and you usually needed a network of people.

Jeff And now.

Emily Now you can just buy a subscription.

Jeff Like Netflix for crime.

Emily More like a highly advanced translation tool. Take the language barrier, for example. Historically, if you were a fraudster in a non-English speaking country targeting a US bank, your phishing emails would be riddled with syntax errors.

Jeff Right, like “Kindly do the needful,” that sort of thing. Super easy to spot.

Emily Exactly. Easy to spot. Now, a fraudster who doesn't speak a word of English can use a large language model to generate perfect, colloquial, corporate American English.

Jeff So the barrier to entry for being a criminal has basically dropped to zero. You don't need skill, you just need an internet connection.

Emily Precisely. It makes the art of fraud cheaper and easier for everyone. And that actually brings us back to that defender's dilemma we mentioned earlier. The banks want to fight fire with fire. They want to use their own AI to stop this, but they're terrified of putting PII personally identifiable information into an AI model.

Jeff Because the rogue factor.

Emily Right? You can't have the banks AI accidentally leaking customer social security numbers into the public domain while it's trying to protect them, or hallucinating and making up fake transactions. That's the definition of irony.

Jeff Absolutely. So we've established the threat is high and the barrier to entry is low. But let's shift gears to where this fraud is actually happening, because we can't talk about the future of banking without talking about the rails. The money actually moves on real time payments or RTP. Yes, the ability to send money instantly. Everyone loves it, I love it. Venmo, Zelle, instant wire transfers. But apparently the fraudsters love it even more.

Emily Speed is the enemy of security. That is the golden rule here. When money moves instantly, it's usually irrevocable. Once it's gone, it's gone. There is no undo button on a real time payment. Right. And David Barnhardt shared a demographic statistic here that I found genuinely surprising. When you think of who falls for scams, who do you usually picture?

Jeff Honestly, I usually think of the elderly like someone's grandmother getting a confusing text message about a package delivery she didn't even order.

Emily And you aren't wrong. Sixty five plus is definitely the highest risk group, but the second most vulnerable group, 18 to 25 year olds. Wait, really?

Jeff The digital natives, the generation that basically grew up with an iPad in the crib, you'd think they would be the most savvy.

Emily You would think so. But it's actually the opposite. Because they are digital natives, they have a massive blind spot. They live their entire lives through their phones. They are so comfortable with the interface that they trust it implicitly. Are they click fast? They swipe fast. They might not perceive when something is incorrect because their muscle memory is just taking over.

Jeff That is a huge vulnerability. So we have instant payments and a user base that clicks before they think. This seems like a recipe for total disaster.

Emily It is. Which actually led to a bit of a controversial opinion among the executives on the panel. They argued that consumers don't actually need real time payments.

Jeff I don't know about that. I definitely feel like I need it when I'm splitting a dinner bill, and I don't want to carry debt for my friends.

Emily Sure, but do you need it in milliseconds or is near real time, say, a five minute delay acceptable if it means you don't get scammed out of your rent money? That's fair. The consensus was that a delay is completely acceptable if it protects the consumer. And this is where Ted dropped one of his well, Tate isms.

Jeff I loved this part. He said friction is the F word.

Emily It's a brilliant reframing in the banking industry. Marketing teams and product teams absolutely hate friction. They want everything seamless, one click, totally invisible. They think friction makes customers leave, right?

Jeff Nobody wants a clunky app.

Emily Exactly. But Ted argued that fraud fighters aren't creating friction just to be annoying. They are putting a lock on the door. You wouldn't say a lock on your front door is friction, would you? You'd say it's security.

Jeff That's a great analogy. I don't complain that my house key takes three seconds to use when I get home.

Emily Exactly. So what is the solution? If we can't stop real time payments and we can't make everyone slow down voluntarily? How do we add that lock without ruining the user experience?

Jeff They talk about throttling, right?

Emily Right. Think of it like traffic lanes on a highway. You treat transactions like cars. The low risk ones, the regular monthly bill payments you always make. They get the express lane go fast. But the risky ones.

Jeff Like a huge transfer to a brand new account at two in the morning.

Emily Exactly. You put that in a slower lane with speed bumps.

Jeff Just enough time to analyze it. Or maybe contact the customer.

Emily Yes, maybe you make them do a biometric check. Maybe you call them. Brian made the point that no payment method has ever scaled without fraud protection credit cards. Zelle. They all had to figure this out eventually. You can't build a highway without guardrails.

Jeff Speaking of building things, let's talk about how the banks are organizing themselves to fight this, because we learned a new acronym in this deep dive.

Emily From fraud and anti-money laundering.

Jeff It sounds like a delicious pastry, like, I'll have a strawberry schrammel and a coffee, but it's actually a huge headache for organizational charts. What is the deal here? Why do these two things need a celebrity couple name?

Emily So traditionally, in almost every bank, these are two completely separate silos. They might as well be on different planets. Fraud teams work in milliseconds. They're trying to stop the transaction now before the money leaves the building. They are the sprinters.

Jeff And AML.

Emily Anti-Money laundering teams are the marathon runners. They work in days, weeks or even months. They're investigating complex schemes after the fact drug trafficking money, terrorist financing. They are filing reports to the government long after the money has already moved.

Jeff Different time zones, different goals, entirely.

Emily Different cultures, different mandates. But the report highlights a massive silo problem. Eighty one percent of firms want a unified approach, but data silos are bottlenecking them.

Jeff When you say data silos, what does that actually look like in practice?

Emily It means the fraud team has a list of bad IP addresses, and the AML team has a list of bad actors. And those lists are in different databases that simply don't talk to each other. So you have two cops chasing the exact same criminal, but they aren't sharing their evidence.

Jeff That seems wildly inefficient. So is the solution just to merge the teams? Just put everyone in one big room?

Emily You'd think so, but the experts actually warned against that. You shouldn't necessarily merge the humans, the investigators, because the actual work is so different. You don't want a sprinter running a marathon, but you must merge the data and the infrastructure.

Jeff Because they're hunting the same bad guys.

Emily And using the exact same data points to do it. Why pay for two different software systems to analyze the same transaction? If you share a single platform, you reduce costs and you get a much better overall picture of the risk. Plus, Brian mentioned a very practical benefit cross training.

Jeff Right. Because fraud comes in waves, doesn't it? It's not a steady stream.

Emily Exactly. Alert volumes are what they call lumpy. Sometimes a specific type of fraud is spiking, like during tax season or Black Friday. And the fraud team is just drowning. If you cross train investigators, you can shift resources to where the fire is burning. Hottest.

Jeff Okay, so we have the threat AI driven fraud. We have the landscape, real time payments. We have the structure framework. Now let's talk about the weapon. The good guys are finally using the AI copilot.

Emily This is a massive pivot in the industry. A few years ago, AI in banking was all about detection models machines deciding yes or no on a transaction. Real black box stuff. Now the excitement is all about investigation assistance generative AI.

Jeff Ted called this removing the yucky part of the job.

Emily And anyone who has ever done data entry or analysis knows exactly what he means.

Jeff Paint the picture for us. What is the yucky part?

Emily Okay, imagine you're an analyst. You get an alert potential money laundering. To investigate that, you have to log in to system A to check the customer's address, then system B to check their transaction history. Then you have to Google the IP address. Then you check a sanctions list. Then you have to copy paste all that into a word document and write a formal report. It's tedious manual data assembly.

Jeff So you're spending ninety percent of your time gathering ingredients and maybe ten percent of your time actually cooking.

Emily Exactly. And that is where the co-pilot comes in. Yinglian Xie shared a stat that frankly blew my mind. She said AI facilitated sa Generation that suspicious activity reports the official documents banks filed to the government can reduce the time to summarize and write reports by ninety five percent ninety five percent.

Jeff That is absurd. That turns an hour of work into what, three minutes?

Emily Think about what that does for an analyst's day. Instead of spending hours typing up a narrative, they spend minutes just reviewing what the AI wrote. They move from being scribes to being decision makers. They can actually use their brains to hunt criminals instead of fighting with formatting.

Jeff But, and I have to play devil's advocate here for a second, is the AI actually good at it? We've all seen AI write weird poetry or just hallucinate facts out of nowhere. If I am a bank, do I really trust a bot to write a legal report to the federal government?

Emily That is the billion dollar question. Brian showed an anecdote about that. Researchers tested models like Claude and Gemini against disguised fraud data. They basically wanted to see if the AI could spot the crime. The result? The AI models were as good as seasoned investigators.

Jeff As good as seasoned investigators. That implies they caught things a junior person might actually miss.

Emily Correct. Because the AI has access to vast amounts of pattern recognition that a human brain, especially a tired human brain at four p m on a Friday, might simply overlook.

Jeff Well, remember the defender's dilemma we started with. Banks are naturally risk averse. They aren't just going to plug ChatGPT into their mainframe tomorrow morning.

Emily No, and they shouldn't. The strategy the panel recommended is eating the elephant one bite at a time. Which means don't start with a customer facing chatbot that might say something crazy to a client. Start with internal investigations. Safe use cases. Use AI to summarize internal notes. Use it to suggest code fixes for the engineers. Test the guardrails there in the back office before you ever let it out into the wild.

Jeff That makes total sense. Build confidence before you build the flashy stuff. Now, looking at the big picture, how do banks even know if they are winning? We used to just look at how much money we lost. But the report suggests moving to a modern success scorecard, right?

Emily Loss is what we call a lagging indicator. If you only look at losses, you're driving down the highway looking in the rear view mirror. You only know you hit something after you've already crashed. The industry is moving toward broader leading metrics.

Jeff Like what specifically?

Emily Operational health. For one, we touched on this, but burnout is a huge issue in fraud teams. It is really hard to keep analysts in seats because the job is high stress and incredibly repetitive. If AI makes the job less yucky, retention goes up. That's a huge win. You keep your institutional knowledge.

Jeff And what about the customer side? I feel like we always talk about the bank's money, but what about my experience for that?

Emily They measure customer friction or the insult rate.

Jeff The insult rate. I have never heard that term before, but I immediately know what it feels like. That's when my card gets declined at the coffee shop and I look like a fool.

Emily Exactly. The bank has insulted you by treating you like a criminal. And the danger. There isn't just that you're annoyed. It's what they call silent defection.

Jeff Silent defection.

Emily Think about it. You don't call the bank and scream at them. You don't cut up the card in a dramatic fit of rage. You just stop using it. You put it in the back of your wallet and you use a different card. That original card just goes dormant. That is a massive hidden cost of aggressive fraud rules. The bank loses the top of wallet status.

Jeff So the fraud team isn't just a cost center anymore. By preventing that, they are actually protecting revenue and enabling growth.

Emily Correct. If you can reduce false positives, basically reduce the insult rate, you are directly helping the bank grow its active account base.

Jeff Before we wrap up today, we have to touch on the final topic because it sounded like something straight out of a Philip K Dick story. Agentic Commerce.

Emily This was the future threat discussed in the Q&A portion. We are moving rapidly toward a world where bots buy things for humans.

Jeff So my AI assistant notices I'm out of milk and just orders it or notices a stock price drop and buys shares or books. My travel for me.

Emily Right. But from a bank's perspective, that scenario is a total nightmare.

Jeff Why is that?

Emily Because banks rely on authentication. Is this really John? If John is using a bot, the behavior changes completely. A bot buys faster than a human. A bot doesn't hesitate. A bot browses differently.

Jeff So do the bank's algorithm. The bot looks exactly like a fraudster.

Emily Exactly. It looks like an automated script. And there is an even deeper question here. How does the bank know the bot has integrity? What if your shopping bot gets hacked? What if a rogue agent starts spending your money without asking?

Jeff It fundamentally changes the question of who is spending the money. It used to be who is the customer? Now it's going to be did the customer authorize this AI agent? And is this agent acting the way it's supposed to?

Emily It really does. It's the next frontier in fraud. We're going to need Kyb know your bot regulations.

Jeff Know your bot. That feels like a whole other deep dive just waiting to happen. So to bring this all home for you listening. We have covered a lot of ground today. The AI paradox, the need for friction frames, copilots silent defection. If you had to distill the final advice from our panel of experts into a single message, what would it be?

Emily I'd break it down by speaker, actually, because they each had a distinct flavor of advice depending on their background. Brian, coming from the consulting side, was all about proactivity. Don't wait for the losses to show up before you fix the hole in the roof. And David David was urgent. Start the AI transformation now. If you wait, the losses from the attacks will eventually cost far more than the transformation itself. It's an investment, not a cost.

Jeff And Ted.

Emily Ted was super practical. Get in the weeds, do proofs of concept. And my favorite part he said make the compliance teams uncomfortable.

Jeff In a safe way. Of course.

Emily Of course, but push the envelope. Don't let bureaucracy stall your defense. If you let the fear of regulation stop you from innovating. The fraudsters win by default.

Jeff And Yinglian had the final word on complexity, didn't she?

Emily She did. She reminded us that all green transactions, the ones that look absolutely perfect, weren't necessarily safe anymore. In an era of pixel perfect fakes and AI driven social engineering, you can't just trust the surface. You have to look deeper.

Jeff That is a seriously sobering thought to end on. Just because it looks right doesn't mean it actually is right.

Emily That's the harsh reality.

Jeff Well, there you have it. The future of fraud is faster, smarter, and a whole lot more complicated. But the tools to fight it are getting better too. Thanks for unpacking this with us. It certainly made me think twice about that next instant payment I sent.

Emily Always happy to help connect the dots.

Jeff And to you listening, here is a question to chew on as you go about your day. If AI can perfectly mimic your voice, your writing style, and even your face on a webcam, what is the one thing that proves you are actually you? Think about that.

Jeff You've been listening to "What the F Happened? Fraud and Financial Crime Deconstructed," a DEFEND podcast by DataVisor. If you want to keep learning between episodes, check out Defend Training, a set of self-paced online courses for fraud and financial crime professionals practical and built around real world scenarios.

Emily And you can earn CPE credits through the ACFE San Francisco Bay Area chapter. You can find it at datavisor.com/defend-training. The link is in the description.

Jeff This episode's audio was generated using Google's Notebook LM based on expert analysis and trusted sources. Thanks for listening. We'll see you next time.