

	EPISODE 33 Analysis The Real-Time Crime Playbook: Why Speed Is the New Fraud Defense AUGUST 24, 2026 <i>This transcript was auto-generated and may contain errors or inaccuracies.</i>
---	--

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.

Emily So imagine you were watching, uh, the most brilliant, highly trained security guard in the world. and they perfectly just flawlessly identified a bank robber from the grainiest blurriest footage imaginable.

Jeff Like a completely perfect identification.

Emily Yes, exactly. The system worked exactly as designed, but they make this brilliant identification while looking out the window watching the robbers plane take off for another country.

Jeff Oh, wow. Yeah, making that perfect, totally accurate decision. Uh. Entirely useless.

Emily Completely useless. Because a correct decision made late is exactly the same as a wrong decision.

Jeff Yeah, that's that's spot on.

Emily And that, you know, brings us to our mission for today. We are doing a deep dive into the real time crime playbook. It's a, it's a 2026 document put out by DataVisor. And it's specifically aimed at fraud and anti-money laundering AML leaders. So our goal today is to really understand why the traditional ways of stopping financial fraud are just failing spectacularly, and how the entire financial world has fundamentally misunderstood the definition of real time.

Jeff Yeah, it's it's wild because we are essentially looking at an invisible war that's happening inside the global financial system literally every second of every day. Mhm. And the stakes, I mean, they couldn't be higher for anyone who interacts with a digital bank account, which is, you know, everyone.

Emily Everyone. Yeah. Okay. So let's unpack this because the playbook starts with a pretty jarring reality check about how fraud programs actually measure their own success, right? Most of these programs, they evaluate themselves almost entirely on accuracy. You know, like, did our system catch the fraud or how many legitimate customers did we accidentally block?

Jeff Right. False positives, false negatives.

Emily Exactly. But the playbook argues that this obsession with accuracy is actually blinding the industry to a massive. Timing problem.

Jeff Yeah. And if we connect this to the bigger picture, it really explains why this shift happened and why things are breaking down now. Because if you think about the old days of banking, um, when you authorized a payment, it didn't actually settle for days.

Emily Right?

Jeff Right. There was this massive slack built into the system. So if a transaction looked risky, the system just put it in a review queue and a human investigator could grab a cup of coffee, open the file on Tuesday morning, and make a decision.

Emily Because the actual money wasn't moving until Thursday anyway.

Jeff Exactly. The queue emptied out long before the money ever left the building.

Emily Wow. Yeah.

Jeff But today, I mean, we live in a world of instant payments. Money clears in seconds, and it moves on irrevocable rails.

Emily Meaning once it's gone, it is gone.

Jeff It is gone. There is no clawback mechanism. So the slack has been completely removed from the financial system. But the fatal flaw is that the old human speed review cuz they still remain.

Emily Which leads to this totally wild situation where the timing failures are actively hiding inside a bank's own metric. Yeah, the playbook points out that a late detection. So let's say the alarm goes off. The model was mathematically right. The investigator worked the case, but the money is already sitting in a different hemisphere, right? That is still counted on the monthly corporate report as a detection win, which.

Jeff Is crazy, right? The operation looks successful on paper while the actual funds were just lost. Yeah. And institutions, they tend to blame the instant payment rails for the losses. They treat instant settlement as some kind of unexpected hazard, rather than the baseline architectural requirement they need to be designing for in the first place.

Emily Right? It's a feature, not a bug.

Jeff Exactly. And when the investigator backlog inevitably piles up, management just treats it like a headcount problem.

Emily Oh, totally.

Jeff They think they just need to hire more people to check the queue faster.

Emily But you cannot throw human headcount at a problem that scales exponentially at machine speed.

Jeff No you can't.

Emily You are just putting more brilliant security guards at the desk to watch more planes fly away.

Jeff That's a great way to put it. It is a profound technical failure, and it's disguised as a staffing issue.

Emily Right. So if accuracy isn't the right metric anymore, how do we actually measure our defenses?

Jeff Well.

Emily The playbook says we have to move away from this illusion of accuracy and face the reality of speed. And they break this down into three specific clocks.

Jeff Yeah. And this is where we move from the theory into the actual mechanics, because there is no single measure of real time. There are three distinct cycles, and they fail entirely independently of one another.

Emily Okay.

Jeff And an attacker only has to beat the slowest one. Oh, okay. So clock number one is the decision clock. This is measured in milliseconds. It is the time from the event happening to the system making a decision. Got it. The target time here is under one hundred milliseconds.

Emily Okay, so that is the clock everyone is talking about when they say real time on a billboard, isn't it?

Jeff Usually, yes. That's the one they advertise. Yeah. But it is only the first hurdle. So clock number two is the adaptation clock. And this is measured in days. It is how long it takes a bank. From the moment they notice a brand new fraud pattern in the wild to actually coding and getting a live control into production to stop it.

Emily Basically making sure they can actually update the locks on the doors when the burglars invent a new lockpick.

Jeff Exactly. It's that reaction time. And then clock number three is the response clock. This is measured in minutes or far worse hours. Oh, wow. This is the time from the system making a decision to an actual action being taken on the account, like freezing the funds.

Emily Okay, wait. Let me push back on this for a second. Sure. Because if I am a massive global bank and I have a super fast state of the art computer system checking transactions in, say, eighty milliseconds. Yeah. Aren't I protected? I mean, eighty milliseconds is incredibly fast.

Jeff You would.

Emily Think so.

Jeff But this introduces what the playbook calls the slowest clock rule. Okay, so the three clocks are sequential. To succeed, the attack has to survive all of them, which means your effective protection is determined by your worst clock, not your best one, right? Yeah. So if your amazing system detects a fraud in eighty milliseconds, but that alert then sits in a human review queue for six hours before anyone physically pushes the blog button.

Emily Yeah.

Jeff You do not have an eighty millisecond program. Yeah. You have a six hour program.

Emily Wow. Okay. And this is exactly why you, the person listening to this right now, need to care about this. Yeah. Because this explains why even the most sophisticated multibillion dollar banks still let consumer scams slip through to your phone. Yeah. The criminals are not outsmarting the computers. They are just exploiting the human speed bottlenecks.

Jeff Exactly. From the attacker's point of view. They just need to pace themselves against human shift workers, not supercomputers. Right. If their attack cycle takes three days and your adaptation clock takes three weeks to write a new rule to stop them, you are perpetually defending against last month's attack.

Emily Wow.

Jeff Detection quality cannot save a system that is fundamentally slower than the threat.

Emily Okay, here's where it gets really interesting. Knowing these clocks is one thing, but the playbook outlines exactly how criminals exploit them in the real world.

Jeff Yeah.

Emily He does. They highlight six specific arenas where crime outruns defense. And it is a fascinating look at the mechanics of modern theft.

Jeff It really.

Emily Is. So the first is irrevocable payments. We touched on this. The money clears instantly. No take backs.

Jeff Right. And without the safety net of a post-transaction review, catching the fraud inside the transaction itself is a structural necessity. It's not a luxury.

Emily Okay. Then you have automated credential and card testing. Criminals unleash bots that test stolen passwords or card numbers thousands of times a minute. Yeah. And the second they hit a threshold that might trigger a block, the bots instantly pivot to new targets.

Jeff And standard velocity rules are utterly useless here.

Emily Right. Why is that?

Jeff Because they are calibrated for human scale mistakes. Like, you know, typing a password wrong three times.

Emily Oh, right. Of course.

Jeff By the time the alarm goes off for a bot testing ten thousand combinations across a network, the viable accounts have already been compromised. Yeah, and they're handed off to the next layer of the fraud ring.

Emily Man. That's crazy. And that flows right into the third arena, which is coordinated burst attacks. Right. Fraud rings do not just hit one account hard anymore. They hit hundreds of accounts simultaneously, and they keep the activity on each individual account just under the warning threshold. So no single profile looks suspicious.

Jeff Yeah, and unless your defense is actively analyzing cross entity correlation meaning? Meaning it is looking at the behavior of the entire crowd in real time rather than staring at one person at a time. Right, right. Unless you're doing that, the attack just looks like normal traffic until the money is gone.

Emily Wow. Okay, so the fourth arena is rapid fun layering. A victim's money is stolen, and within minutes it is chopped up and moved through a massive network of meal accounts.

Jeff Yeah, the mules.

Emily Hopping across different banks and different payment rails to basically scramble the trail.

Jeff And old batch processes fail catastrophically here because an AML system running a batch process overnight, it might successfully flag the mule network the next day. Right. But you haven't recovered any money. No. You have just generated a very expensive compliance document for the regulators.

Emily Literally just doing paperwork at that point.

Jeff Exactly.

Emily Okay. Arena five is real time social engineering. And this is terrifying. We are talking about coercion happening live on the phone. Yeah. The fraudster is talking to the victim, convincing them to wire their life savings. And because the victim is the one actively authenticating. Yeah, typing their real password on their real phone from their real house. The normal checkpoints just wave them right through the system. Thinks looks like John acts like John. Must be John, right?

Jeff Those traditional checkpoints, they fail by design in coercion scenarios because they're designed to let the real person in. So to stop that, the system has to analyze behavioral and session anomalies live in the moment. It has to realize John is hesitating or, you know, swiping differently or on an active phone call he doesn't usually make while transferring large sums.

Emily Yeah. Looking at the how, not just the who.

Jeff Exactly.

Emily Okay, the sixth arena is the one that really got me same session account takeover.

Jeff Oh yeah.

Emily Let's walk through just a thirty second horror story to understand how bad this is. Picture this. You click a bad link in a text message.

Jeff Which happens all the time.

Emily All the time. And in one continuous, unbroken session, a bad actor logs in with your stolen password, swaps your registered device to their phone, changes the email address on file so you don't get alerts and immediately wires the maximum limit out of your account.

Jeff Yeah. Boom. It's gone. And looking at these six arenas, the common thread is undeniable. Every single one of these attack vectors bypasses security controls that look at events in isolation or rely on delayed batch processing. If a bank's system evaluates a changed email address during a Monday night batch run and then evaluates a large payout on a Tuesday morning batch run.

Emily It completely misses the context.

Jeff Exactly. But if a system sees those actions happening back to back in the exact same minute, the fraud is glaringly obvious.

Emily Because criminals are operating at light speed. They are looking for those blind spots. And naturally, if you go to any security vendor today, every single one of them claims to offer real time protection.

Jeff Oh, of.

Emily Course they have it plastered in giant letters on their websites, but the playbook comes out swinging. Here, it warns that these real time claims are often a complete technical illusion.

Jeff Yeah, it is the mirage of real time, because it might be true in a strictly literal, narrow engineering sense, sure, but it is completely useless in practice. And the playbook identifies three specific gaps where these vendor claims just fall apart under pressure.

Emily Okay, so gap one is stale features, and I love this one because it is so deceptive. It is basically like using yesterday's newspaper to predict today's weather.

Jeff That's a great analogy, right?

Emily Because the vendor will proudly say, look, our model returns a risk score in just forty milliseconds. And it does. Yeah, it does, but the data it is using to make that forty millisecond decision, you know, the behavioral baselines, the cross-channel aggregates, that data was pre-calculated overnight.

Jeff Exactly. The scoring mechanism is real time, but the intelligence feeding it is not. Right. So if an attacker changes tactics at two point zero p m and your forty millisecond model is using a data profile aggregated at three point zero a m. You are utterly blind to the attack.

Emily You're just totally exposed, okay? Gap two is the degraded fast path, and I'm struggling with this concept a bit. If I am a massive global bank with, you know, essentially unlimited resources, why can't I just buy bigger servers? Why am I forced to drop complex tasks just because it's Black Friday or there's a volume spike?

Jeff Because legacy on premise architecture has hard physical limits. I mean, you can only squeeze so much through those pipes, okay? When those old systems get hit with a massive spike in transaction volume, they simply cannot process the load and still meet their speed guarantees. So they have a built in safety valves. They start dropping the heavy, complex analytical tasks.

Emily Like what?

Jeff Like they skip checking the deep relationship graphs, or they route the transaction to a dumber, lighter model just to get it out the door faster.

Emily So they're essentially lowering their shields to accommodate the traffic.

Jeff Yeah. It is an incredibly dangerous design compromise. Yeah. The fastest decisions end up being the least informed. Decisions.

Emily Oh, wow.

Jeff And those coordinated burst attacks we talked about. They are specifically designed to trigger those volume spikes.

Emily Wait. Really?

Jeff Oh, yeah. The criminals forced the system to lower its shields, and then they strike.

Emily Unbelievable. Just engineering a stampede. So the guards give up.

Jeff Exactly.

Emily Wow. Okay. And gap three is batch response, which we kind of touched on with the slow clocks. Yeah. You get a genuinely fast, accurate detection, but the system doesn't have the authority to automatically block the transaction. It just generates an alert and jumps it in a queue for a human to review.

Jeff Right. So your multi-million dollar technology stack is suddenly bottlenecked by who called in sick for the afternoon shift.

Emily It's just so absurd. Yeah. So if everyone is faking it with overnight data or degrading their fast paths under load, what actually has to happen inside that tiny one hundred millisecond window for it to be true real time?

Jeff Yeah, that's the big question.

Emily The playbook uses this analogy that handling a transaction in one hundred milliseconds is basically like operating a nightclub door.

Jeff What's fascinating here is how well that analogy maps to the heavy lifting required behind the scenes, because real time is essentially a latency budget. Okay. And a true system has to fit six distinct stages into it. So stage one, in the time it takes the person to hand you their ID, you have to ingest and unify the event data with internal and third party signals as it arrives.

Emily Right. And then stage two, you have to make sure it's not a fake ID. Exactly. You resolve the identity, you match that event to a specific customer device and counterparty across all your channels.

Jeff Yeah. And then stage three is where the legacy systems really fail. You have to compute features in flight.

Emily In flight. Okay.

Jeff Meaning no pre-aggregated overnight data. You calculate the behavioral and velocity features on the live event itself.

Emily So in the nightclub analogy, this is checking if they just got kicked out of the club next door five minutes ago.

Jeff Yes, exactly. You need to know what they did five minutes ago. Not yesterday. Right then. Stage four is the graph traversal.

Emily Oh, right. So you have to see if they arrived with the guy who started a bar fight last week. Right? You traverse the relationship graphs looking for hidden connections to known fraud rings.

Jeff Spot on.

Emily Yeah.

Jeff And only after all of that do we reach stage five, where you finally score and evaluate the data. Wow. And then stage six, you actually decide and act. You block it, you allow it, or you hold it. And all of that has to happen under one hundred milliseconds.

Emily So if stages one through four break down, like if you can't ingest the data quickly or resolve the identity or compute the live features or check the graph, yeah, the whole system fails. It doesn't matter how fast the scoring model in stage five is, if the data feeding it is garbage.

Jeff Exactly. But vendors, they love to quote their speed for stages five and six because scoring and acting are the easy parts, right? But stages one through four are where the war is actually won or lost. Those are profound architectural challenges. You cannot simply tweak a setting to fix a system that fundamentally relies on overnight batch data.

Emily It has to be built differently from the very foundation.

Jeff It has to be rebuilt entirely.

Emily Okay, so we have thoroughly torn down the legacy systems and the fake real time claims. And honestly, it sounds pretty grim out there.

Jeff Yeah, it's a tough landscape.

Emily But what does the DataVisor playbook say actually works? How do institutions actually close this gap?

Jeff Well, the playbook provides a really comprehensive blueprint for building true end to end, real time defenses, and it directly addresses those architectural flaws we just walked through.

Emily Okay. So if the core issue is that our models are using yesterday's data, the only real solution is to calculate those behaviors right at the moment of the swipe, right. And the playbook calls this in-flight computation. You have to convert the system. So it is calculating behaviors velocities and risk on the live event itself just abandoning the overnight data stores entirely.

Jeff Yeah. And that is the highest leveraged change in organization can make. It is literally the dividing line between a system that is actually real time and one that just looks real time on a marketing brochure. Right?

Emily Okay. And to fix the degraded fast path problem where systems lower their shields under heavy load. Yeah. The blueprint insists on keeping full analysis inside the budget. You refuse to make that dangerous trade off. You never drop your graph traversals just because volume spikes.

Jeff And the only way to achieve that is through elastic cloud native infrastructure.

Emily Okay.

Jeff Because when a burst attack hits, an elastic cloud system instantly spins up more server capacity to handle the load.

Emily It just expands to meet the need.

Jeff Exactly. It makes handling massive spikes a matter of raw, flexible computing power, rather than forcing the system to dumb down as models to survive the traffic.

Emily That makes so much sense. And then to eliminate that agonizing response clock, you have to put automated action directly in the decision path. Yes. Stop relying on human shift coverage to physically hit the block button for obvious fraud.

Jeff Right. And to be clear, the objective isn't to replace human investigators. The goal is to auto decision the high confidence fraud.

Emily So you block the obvious attacks instantly and automatically.

Jeff Exactly. Which frees up your human investigators to tackle the truly complex edge cases that actually require nuance and judgment.

Emily Yeah. Stop making them click block on obvious bot traffic. Exactly. Now, the blueprints approach to the adaptation clock is just wild. It's amazing because remember, that's the clock that takes days or weeks to get a new rule into production. Right. The playbook suggests using generative and conversational AI agents so fraud teams can analyze a new pattern, build a rule, test it against historical data, and deploy it to production in minutes. Yeah. You are turning a weeks long IT release cycle into a quick conversation with an AI.

Jeff And that staggering compression of time completely flips the advantage back to the defender. You are no longer defending against last month's attacks.

Emily Yeah, you're actually fighting the fire while it's burning. Yes. The final piece is triaging at speed, because if you have real time detection working perfectly, it is going to generate a massive volume of alerts.

Jeff Oh, absolutely.

Emily So you use AI triage to prioritize and explain those alerts, automatically gathering all the context an investigator needs, which the playbook notes cuts investigation time by twenty to thirty times.

Jeff And that ensures your human response clock doesn't just become the new catastrophic bottleneck once you have successfully modernized the underlying technology.

Emily Right. Okay. So if I'm a skeptic listening to all this, I am obviously asking for proof. Sure. Does this actually work at the scale of global finance? But you look at the numbers DataVisor provides in the playbook, and they are processing over thirty billion events daily. Yeah. They are hitting those decision clocks of under one hundred milliseconds while processing more than fifteen thousand queries per second.

Jeff And crucially, that is fifteen thousand queries per second with full in-flight feature computation and deep graph analysis.

Emily Wow.

Jeff There are no degraded fast paths. There are no lowered shields.

Emily That is wild. And there are testimonials in there from organizations like NASA, Federal Credit Union saying they are now deploying brand new fraud strategies in just five minutes. A firm discusses seamless integration into their massive transaction flow, and DataVisor also highlights their position as a leader in the Q2 twenty twenty five Forrester Wave for AML solutions. Yeah. So what does this all mean for someone running one of these programs? The playbook ends with a ninety day plan. And honestly, it is so refreshing because step one is incredibly straightforward.

Jeff Do not buy anything yet.

Emily Exactly. Do not buy anything yet.

Jeff Yeah. The first phase is purely diagnostic. You have to audit your own existing features. You rigorously measure your own three clocks. So the decision adaptation and response clocks, right? You basically have to prove to yourself exactly where your architectural bottlenecks are before you can even begin to fix them.

Emily Yeah, that makes a lot of sense. So as we wrap up this deep dive, you know, this is not just a technical manual for bankers. No, this is really a blueprint for understanding the invisible shield that is supposed to be protecting our daily digital lives. We live in a world of instant, irrevocable money. Yeah. And the defenses protecting that money have to be deeply, architecturally fast, not just tuned to look fast on a quarterly report.

Jeff Absolutely. Though this raises an important question, though. We discuss how the playbook uses AI to compress the defenders adaptation clock, taking it from days down to five minutes to write and deploy a new defensive rule.

Emily Right?

Jeff That is incredible progress. But if we connect this to the broader trajectory of technology, what happens when the attackers start plugging those exact same large language models and conversational AI into their bot networks.

Emily Oh wow. I hadn't even thought of that.

Jeff Right? Right now we celebrate that a human fraud analyst can converse with an AI to write a new defensive rule in five minutes. But what happens tomorrow when the attackers can autonomously rewrite their entire evasion strategy, probing for new weaknesses in five seconds?

Emily Jeez.

Jeff We have successfully solved the human speed bottleneck on the defense side. Sure, but the next war, it will not be humans versus bots. It is going to be algorithm versus algorithm.

Emily Algorithm versus algorithm. Wow. It really makes you think back to our brilliant security guard staring at the monitors. Yeah. Only next time they won't just be watching a single plane take off. They'll be watching a fleet of drones instantly rerouting themselves a thousand times a second, learning from every blocked attempt in real time, and wondering how on earth they're supposed to catch them all.

Jeff It's definitely something to chew on.

Emily Something to keep in mind the next time you hit send on a payment.

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.