EPISODE 26 | Reports

Forrester Trend Report - Managing AI Agent Commerce

JULY 06, 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.

Emily When you picture getting scammed or, you know, having your financial information stolen, you probably picture a very specific, uh, very human scenario, right?

Jeff Like a one on one interaction.

Emily Exactly. It's like the person looking over your shoulder while you type in your pin. Or maybe it's the digital version of that, right? A hacker sitting in a basement somewhere, manually testing passwords or, you know, trying to trick you into clicking a phishing link in your email.

Jeff Yeah, we definitely tend to think of fraud as this battle of wits between you and, well, another human being.

Emily Right. And that human element is central to how we've historically understood crime, because there is always a physical bottleneck on the other end.

Jeff Absolutely. I mean, it takes actual time for a person to steal data, decide how to use it, navigate a website and, you know, process that stolen info into cash.

Emily You have to type, they have to click exactly.

Jeff The attacker has to sleep, they make mistakes and they just have physical limits on how many targets they can hit at once.

Emily But consider what happens when you remove that human limitation entirely. Like what if the entity trying to drain your account or hijack your transactions isn't a person at all?

Jeff Which is a terrifying thought.

Emily It really is. Imagine an attacker that is just, you know, a piece of self-executing code. No physical body, no need to sleep. And it has the ability to simultaneously test every digital lock on thousands of websites in like a fraction of a second.

Jeff You wouldn't even realize an attack had started before it was already over.

Emily And the money was just gone.

Jeff Yeah. And that changes the entire nature of the threat. We stop looking at fraud as a targeted manual strike and start having to treat it almost like an environmental hazard.

Emily Wow. An environmental hazard. That's a good way to put.

Jeff It, right? Because when the attacker is purely algorithmic, the landscape of digital security transforms practically overnight.

Emily And that brings us to why we're here. Welcome to today's deep dive. We are spending some time today looking closely at that exact transformation for you.

Jeff It's going to be a fascinating one.

Emily Oh, definitely. We are pulling apart a brief but incredibly dense Trend report from Forrester.

Jeff And it's titled Managing AI Agent Commerce Fraud.

Emily Right. And it's a compelling piece of research because it isn't focused on like the phishing scams of five years ago. It is looking squarely at the immediate future.

Jeff Yeah, predicting how the tools we are building for our own convenience are going to be weaponized against us.

Emily So our mission today is to explore this high speed collision between automated convenience and automated crime, keeping you, the listener, ahead of the curve.

Jeff It's a critical topic right now.

Emily It really is, because the core premise of the Forrester Report asks a crucial question about modern commerce. It asks what happens when the entity committing the fraud is what they call a runaway malicious AI agent.

Jeff That phrase alone is pretty chilling. Runaway malicious AI agent.

Emily Seriously. But before we get into how an autonomous piece of code actually commits a crime, we need to understand the baseline, right? We have to look at why these AI agents are authorized to operate in the commerce space to begin with, right?

Jeff Because we put them there.

Emily Exactly. The report points out that AI agents are increasingly being trusted with three specific tasks first, discovering products and services. Second, making e-commerce purchases on our behalf.

Jeff And third, performing consumer services.

Emily Right. And the specific example they use for that last one is, uh, making restaurant reservations.

Jeff Which I mean, those sound like perfectly benign everyday tasks. Yeah. And they're meant to be. The whole goal is removing the friction from our daily chores.

Emily Okay, let's unpack this because I want to break down how that actually looks in practice. Think about, you know, planning a nice dinner at home. It's one thing to ask a conversational AI to generate a recipe for like authentic lasagna.

Jeff Sure. We've been using language models for that kind of brainstorming for a while now, right?

Emily That's just text. But we are crossing a new threshold when you can say to your digital assistant, hey, here is access to my bank account, go find the best prices for imported San Marzano tomatoes and fresh pasta across all local grocery stores. Buy them, arrange the delivery, and then.

Jeff Book a table.

Emily Right? Yeah. Book me a table for two at that exclusive Italian place downtown for next Friday. Think of this AI as the ultimate hyper efficient personal assistant who never sleeps.

Jeff It's a huge leap in trust.

Emily It is. You are delegating actual financial agency, the ability to spend your money to a piece of software. So I have to ask, how does this shift where the shopper is an algorithm rather than you or me, change the fundamental mechanics of e-commerce?

Jeff Well, what's fascinating here is that it alters the volume and velocity of commerce at a foundational level.

Emily How so?

Jeff Well, when you or I shop for those lasagna ingredients, the process is incredibly slow, right? We open a browser, we wait for the page to render the images. We scroll, we read reviews.

Emily We get distracted by a text message.

Jeff Exactly. We get distracted. We add things to a cart, and then we have to manually type in a credit card number. Human existence is just full of friction.

Emily We second guess ourselves too. Like, I'll abandon a cart just because I don't feel like getting up to find my wallet across the room.

Jeff Right? We've all been there. But an autonomous digital assistant, it executes its parameters instantly. It doesn't need a website to render flashy banner ads or, you know, nice typography.

Emily Because it's not looking at the screen.

Jeff Exactly. It interacts with the store's database directly. It can scrape the inventory of fifty different grocery stores, calculate shipping costs, apply active coupon codes, and execute the payment in milliseconds.

Emily Wow. Milliseconds.

Jeff Yeah. And the broader implication here is that commerce is shifting away from purely business to consumer or B2C. We are entering an era of business to AI.

Emily Business to AI. I mean, that implies a complete redesign of how the internet works.

Jeff It absolutely does. The storefront isn't trying to appeal to human psychology or impulse buying anymore. It's optimizing to interface with machine logic.

Emily That makes total sense. And I guess you see it with the restaurant reservations the report mentioned, too, like a digital agent doesn't dial a phone number and sit on old listening to elevator music.

Jeff No, not at all. It pings the restaurant's booking system via an API, an application programming interface. The machines literally talk directly to each other.

Emily So it's seamless.

Jeff Seamless, and instantaneous. But and this is the crucial part, that exact removal of friction, the speed that makes it so convenient for you to get a table is exactly what creates the mass of vulnerability, right?

Emily Which brings us to the dark side of delegating our wallets to algorithms. Because if digital engines are out there making autonomous transactions at lightning speed, the sheer scale of global commerce just explodes.

Jeff It scales up massively.

Emily And Forrester issues a very explicit warning about this new environment. They state that curbing fraud during these automated transactions is critical because, and I'm quoting the report directly here, runaway malicious AI agents can cause more trouble and losses faster than human fraudsters.

Jeff Yet that speed differential is the crux of the entire problem. It's what separates this from traditional cybercrime.

Emily Here's where it gets really interesting, though, because I want to challenge that slightly.

Jeff Okay, go for it.

Emily Let's look at the mechanics of fraud as we understand them today. If a human scammer steals my credit card info, they might try to buy, say, a few expensive laptops, right?

Jeff Classic fraud.

Emily But my bank has fraud detection limits, right? If they see three laptops being purchased in five minutes, they freeze the card. They send me an SMS alert.

Jeff Yep. The standard safeguard.

Emily So if a malicious bot tries to buy ten thousand laptops in a millisecond, wouldn't those exact same banking limits just block it instantly? I guess I'm asking, is the main threat here simply the speed of the AI, or is it the sheer lack of human bottlenecks that makes it so dangerous? Why is the speed actually a new unmanageable threat if institutions have volume caps?

Jeff If we connect this to the bigger picture, that is a crucial distinction to make. You're thinking of like a brute force attack where a bot just hammers one stolen credit card until it hits a wall, right.

Emily Which the bank would catch.

Jeff Exactly. But a sophisticated autonomous attack bot doesn't act like a human scammer on fast forward. It acts intelligently to subvert the rules. It knows those volume caps exist.

Emily Wait, really? So how does it bypass them if it knows they're there?

Jeff But distributing the attack, a malicious agent might compromise a database and extract ten thousand different credit card numbers at once. Okay. And instead of trying to buy a massive red flag item like a laptop, the bot programs itself to execute ten thousand individual micro transactions across hundreds of different websites simultaneously. Oh, wow. Yeah, it buys a three dollars digital gift card here, a five dollars software license there. Every single transaction is kept deliberately under the threshold that would trigger an automatic bank freeze.

Emily So it basically.

Emily Just blends in with the noise of normal everyday purchases.

Jeff Yes, exactly. It looks like normal traffic. And because it operates autonomously and instantly, by the time a human analyst at the bank notices a statistical anomaly in the broader system, say they notice an unusual spike in three dollars purchases across their network, the bot has already finished the entire operation.

Emily It's just gone.

Jeff Gone. It is executed. The purchases transferred, the digital assets to a secondary market, laundered the funds, and deleted its own tracks. The loss is realized before the human defense even boots up. And that is exactly what Forrester means by more trouble and losses faster.

Emily That is wild.

Emily And I imagine this applies to things outside of just stolen credit cards too, right?

Jeff Oh, definitely.

Emily Like going back to the restaurant reservation example from the report. I think anyone who has tried to get tickets to a major concert recently knows the pain of bots buying up the inventory.

Jeff Oh yeah. The reservation ecosystem is incredibly vulnerable to this. A malicious bot could ping the API of every high end restaurant in a major city. The literal second reservations open for the month.

Emily Or scoop them all.

Jeff Up.

Jeff Yep, it books every available table for prime dining hours using synthetic fake identities.

Emily And then the human stammer behind the bot turns around and sells those reservations on a secondary market for a massive markup.

Jeff Exactly.

Jeff And the restaurant suffers because they have empty tables. If the reservations don't sell to real people, and the consumer suffers because they can't get a table without paying a ransom, right.

Emily And this highlights why Forrester uses the specific term runaway. A malicious algorithmic agent operates without physical constraints.

Jeff Not at all.

Emily Like if a human runs into a hurdle, say, a, t, c, h s asking them to identify traffic lights, they slow down. It takes a few seconds.

Jeff But modern malicious code is increasingly designed to solve or bypass those roadblocks automatically.

Emily Yeah, it can spoof different IP addresses to make it look like the requests are coming from different countries. It adapts its autonomous self-executing destruction. The human defender is just entirely outpaced, completely outpaced. So if the human is outpaced and the self-executing bots can bypass our traditional tripwires, how do we actually defend the ecosystem? What does the roadmap for fighting back look like in this report?

Jeff Well, the Forrester report provides a very specific framework for them. They argue that to curb these rapid losses, businesses have to implement dedicated fraud management solutions.

Jeff Okay.

Jeff And they divide these into two distinct categories technical defenses and non-technical defenses.

Emily So what does this all mean? I want to dig into that division because frankly, my initial assumption is that if we are facing a highly technical algorithmic threat, the only logical response is a highly technical defiance.

Jeff Right? I think so, yeah.

Emily Like we need to build a better, faster defense algorithm to fight their attack algorithm. Do we not just need more advanced AI to protect the system? Why does the report explicitly highlight non-technical defenses to.

Jeff This raises an important question because technical defenses are absolutely the baseline. You cannot process data at the speed these malicious agents are attacking without advanced machine learning on your side, right?

Emily You need AI to fight AI.

Jeff Exactly.

Jeff You mentioned earlier how a human typing a credit card is slow and full of friction. Technical defenses capitalize on that. A fraud management system will use behavioral analytics to measure exactly how a user is interacting with a website.

Emily Okay, so it's looking at things beyond just the password getting typed in correctly.

Jeff Much deeper. It measures the trajectory of the mouse cursor. It measures the dwell time, like how many milliseconds the user pauses before moving to the next text field.

Emily Oh wow. It measures typing cadence, too.

Jeff Yes, typing cadence is huge. If a storefront detects that a user navigated three complex web pages, filled out a twelve field checkout form and submitted payment in zero point zero four seconds.

Jeff Which.

Emily Is impossible.

Jeff Right?

Jeff The technical defense flags that as physically impossible for a human. It recognizes the machine logic and blocks a transaction instantly.

Jeff And.

Emily I'd imagine this requires immense computing power, which is where specialized AI tools come in.

Jeff Precisely.

Emily Okay, so the technical side makes complete sense. We use defensive AI to spot the physical impossibilities of the attacking AI.

Jeff Right.

Emily But that brings me back to the second category of the report emphasizes which is non-technical defenses. on the surface, fighting a cutting edge algorithmic threat with non-technical solutions. Sounds like bringing a rule book to a knife fight.

Jeff It does sound counterintuitive. Yeah.

Emily Why does Forrester place non-technical strategies, which I assume means like manual policies or business rules on equal footing with software solutions.

Jeff Because if you rely.

Jeff Exclusively on software to fight software, you are trapping yourself in a perpetual arms race.

Emily Are the attacker builds a better bot. So we build a better firewall so they build a better bot.

Jeff Exactly.

Jeff And in that arms race, the attacker has a massive advantage. They only need to find one single logic flaw in your tactical defense to break through.

Jeff Just one. Just one. Yeah.

Jeff And because they operate at machine speed. Once they find that single flaw, they could exploit it ten thousand times a minute before your engineering team even realizes the firewall needs patching.

Emily That's terrifying.

Jeff It is.

Jeff Technical defenses are brittle if they stand alone. That is why non-technical defenses are critical A non-technical defense doesn't try to out calculate the bot. It changes the economic rules of the game.

Emily Oh I see. This reminds me of how physical security works. Like if you are building a bank, you install the high tech alarm system, right? You have the laser grids, the motion sensors, the digital keypads.

Jeff Right. That's your technical defense.

Emily Exactly. But you don't stop there. You also implement a non-technical defense, like a strict policy that the main vault requires two different bank managers to insert two physical keys at the exact same time before it opens. Yes, the alarm system is designed to catch the speed of the break in, but the policy is what actually prevents the catastrophic loss of the money.

Jeff That is an excellent way to frame it. You're using structural policies to dictate the terms of engagement. Let's map that back to the restaurant reservation bots we talked about. Okay. We established that the

technical defense might look for an IP address making requests too quickly, but a smart, malicious agent just spoofs a thousand different IP addresses, right?

Emily It roots itself through servers all over the world to look like a thousand different people booking tables.

Jeff Exactly. So the technical defense fails. But what if the restaurant implements a non-technical defense? What if they changed their booking policy to require a nonrefundable twenty dollars deposit just to hold a table?

Emily Uh, that changes the math completely.

Jeff Completely. The malicious bot is perfectly capable of bypassing the IP block and navigating the booking form, but the scammer running the bot doesn't want to actually spend twenty dollars of real money for every fake reservation.

Emily No, because they might not make it back.

Jeff Exactly. If they instruct the bot to hoard a thousand tables, they suddenly have twenty thousand dollars in sunk costs and they might not be able to resell all those tables. The non-technical policy breaks the economic model of the fraud. It introduces artificial friction that ruins the attacker's return on investment.

Emily That makes perfect sense. The bot is fast, but it can't outrun a bad business model. Are there examples of this in the e-commerce space too? Like where physical or digital products are involved?

Jeff Definitely consider the purchase of digital gift cards. Okay. That's a favorite target for malicious bots because the delivery is instant and the asset is super easy to launder. A non-technical defense would be a store policy, instituting a mandatory twenty four hour holding period on the fulfillment of all digital gift card purchases.

Emily Ah. So regardless of how quickly the transaction was approved by the credit card processor, you wait.

Jeff Exactly. So even if the attacking algorithm successfully bypasses the behavioral analytics, mimics human mouse clicks perfectly, and uses a stolen credit card to buy a thousand dollars in gift cards.

Emily They don't actually get the cards.

Jeff They don't get the cards for a full day. And that twenty four hour window is critical. It provides enough time for the actual human victim to wake up, check their email, see the fraudulent receipt, and call their bank to issue a chargeback.

Emily It dictates the pace of the fallout.

Jeff Yes, the malicious agent is designed for instant smash and grab operations by implementing a non-technical holding policy. The business denies the attacker the instant gratification their entire model relies on.

Emily You are intentionally reintroducing the friction that the AI was originally designed to eliminate.

Jeff Yes, exactly. A truly robust fraud management solution has to be a hybrid. You blend the software guardrails, the technical defenses that process data at high speed with structural non-technical rules that remove the incentive or the capability for runaway damage.

Emily You design the ecosystem so that even if a self-executing code slips past the AI censors, it immediately slams into a brick wall of policy.

Jeff Spot on.

Emily Well, this has been a deeply illuminating look into a very complex, fast moving space. To synthesize the core takeaways from the Forrester Report for everyone listening, we are entering a highly convenient era of business to AI.

Jeff We really are.

Emily Digital agents will increasingly handle the friction of our daily lives, from scraping the web for the best price on groceries, to interfacing with booking APIs so we can get a table on a Friday night.

Jeff But that same automated ecosystem is exactly what enables the runaway malicious AI agent. The same technology that makes shopping instant makes theft instant.

Emily Right? And because these autonomous threats lack human physical limitations, they can execute thousands of microtransactions, bypass traditional volume caps, and cause immense financial losses before a human analyst even registers the attack.

Jeff It's a daunting reality.

Emily It is. And to defend against this, organizations can't just rely on an endless algorithmic arms race. They have to implement layered fraud management solutions utilizing advanced technical tools for real time detection, backed by non-technical policies that disrupt the economic incentives of the attackers.

Jeff You know, it forces us to reconsider what our digital landscape is actually becoming.

Emily What do you mean?

Jeff Well, we started this deep dive talking about the very human element of getting scammed. Right. The pickpocket. The hacker at a keyboard. But look at the trajectory we've just outlined. If autonomous digital agents are increasingly the entities making our purchases and interacting with storefronts, and if highly advanced AI systems are the entities analyzing behavior and defending the gates against malicious bots.

Emily Where does the human fit into this picture?

Jeff Exactly. Are we rapidly approaching an e-commerce ecosystem where humans are entirely cut out of the loop? It raises the possibility that we are destined to become mere bystanders. We might just find ourselves sitting back watching our bank accounts, while an invisible, high speed digital battleground of algorithms buys, attacks and blocks each other in the background.

Emily Just machines, fighting machines, right?

Jeff The pickpocket is code, the security guard is code, and the shopper is code. We merely provide the capital.

Emily That puts a completely different spin on the idea of automated convenience. Something to really think about. Thank you for joining us on this deep dive into the evolving mechanics of AI commerce fraud. We will see you next time.

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.