EPISODE 31

Why Credit Unions Are Becoming Fraud's Favorite Target — and How They're Fighting Back

AUGUST 10, 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 You know, it's, uh, it's actually kind of funny to think about how you interact with your phone these days.

Emily Oh, totally.

Jeff Like you find a hilarious meme, you drop it into a group chat and instantly your friends on the other side of the country are just cracking up. It's completely effortless, right?

Emily It's just muscle memory at this point.

Jeff Exactly. But here's the crazy part. Sending one thousand dollars to a contractor or, you know, splitting a massive dinner bill with a friend uses almost that exact same effortless motion. Yeah. A couple of taps on Zelle, Venmo, or E-transfer. And the money is just, it's just there. And we take that instantaneous magic completely for granted.

Emily We really do. I mean, we've come to expect that our finances should move at the exact same speed as our text messages, right? The friction is just entirely gone from the user experience, which, you know, it feels like a massive technological triumph.

Jeff It does. But our mission for this deep dive today is to explore the dark side of that disappearing friction.

Emily Yeah, it's a big topic.

Jeff We're pulling from a really eye opening interview on the Credit Union Connection featuring Dr. Yinglian Xie. She's the Co-founder and President for technology at DataVisor.

Emily And her core warning in this discussion is that while instant payment rails are incredibly convenient for us.

Jeff So convenient.

Emily Right? But they have essentially created a hyper speed express lane for high tech heists.

Jeff Oh wow. So the very thing that makes the system so incredibly useful for you and me is what makes it like a playground for bad actors.

Emily Precisely. And the central dilemma we're looking at here is how smaller and mid-sized financial institutions like your local credit union can possibly protect your money against these highly sophisticated AI powered scammers.

Jeff Without bankrupting their own IT departments in the process?

Emily Exactly. Or, you know, ruining that smooth user experience we all love.

Jeff Okay, let's unpack this mechanics wise first, because we all love the convenience of real time. But why does that exact speed suddenly make the infrastructure of money so incredibly fragile?

Emily Well, it really comes down to the window of intervention. I mean, historically, the financial system had these built in delays.

Jeff Like processing time.

Emily Right? Think about a traditional batched ACH transfer. The automated clearinghouse system. When you initiated a transfer, your bank didn't actually send the money right then and there.

Jeff Oh, right. They gathered them all up.

Emily Exactly. They gathered up thousands of transaction requests over the course of the day, put them into a massive digital batch file, and then sent that file to the Federal Reserve overnight to be cleared and settled.

Jeff Over the next day or two, usually.

Emily Yeah, exactly.

Jeff So the delay wasn't just old technology being slow. It was functionally a cooling off period.

Emily That's a great way to put it.

Jeff If a fraudster compromised an account and initiated a transfer on a Tuesday morning. Human investigators had a multi-day buffer, right? They could run reports spot anomalies, flagged the transaction and literally stopped the money before it actually left the building on Wednesday.

Emily But real time payments completely obliterate that buffer. Instantaneous settlement means that when you hit send on a newer form of payment, the funds clear and settle in the receiving account in milliseconds.

Jeff Milliseconds.

Emily There is no taking it back. If a legacy fraud detection system takes even 30s to query a database.

Jeff They've already gone.

Emily Right. They analyze a transaction, realize it's fraudulent, and the battle is already lost. The fraudster has the money and has likely already moved it again.

Jeff Usually into cryptocurrency, right. Or offshore accounts.

Emily Exactly. Places where it just can't be clawed back.

Jeff So since megabanks have the massive infrastructure to try and spot these instant attacks, the fraudsters are forced to look for blind spots in the ecosystem.

Emily They go where the resistance is lowest.

Jeff And that pushes them downstream because, according to Dr. Xie scammers aren't prioritizing the massive global mega banks right now.

Emily No they're not.

Jeff They are specifically targeting mid-sized banks and credit unions, basically viewing them as soft targets.

Emily Which is terrifying for those smaller institutions.

Jeff Our credit unions basically acting like a friendly neighborhood store that just, you know, leaves its doors wide open to keep the customers happy. Are they being penalized for being too nice?

Emily Well, credit unions fundamentally differentiate themselves through member experience. I mean, their entire brand identity is built on a personal connection, low friction, and being incredibly member friendly. Right. They want it to be as easy as possible for you to log in and move your money and go about your day without jumping through six different security hoops, which.

Jeff Is why people love him. You don't feel like just a number in a database. You feel like part of a community.

Emily Exactly. But the attackers know this. They assume that to maintain that low friction environment, a credit union might have fewer security hurdles.

Jeff They exploit the trust.

Emily . Yeah, but the vulnerability isn't just about being overly accommodating. It's structural. How so? Smaller institutions simply have fewer staff, tighter security budgets, and fewer operational reviewers to manually check suspicious activity.

Jeff Oh, sure. Compared to a massive institution like Chase or Bank of America.

Emily Right. But a lack of manpower is one thing. The sources point to a massive data deficit being the real danger here.

Jeff A data deficit. What do you mean?

Emily Think about how modern fraud detection works. It relies on recognizing patterns. A megabank processes millions of transactions an hour.

Jeff So they see everything.

Emily Exactly. If a new sophisticated fraud ring starts testing a novel attack method, the megabank systems will see that attack attempted hundreds of times across different accounts within minutes. Oh, wow. They have a massive pool of data to quickly identify the footprint of the attack, learn from it, and update their defenses. A local credit union, on the other hand, might only see one or two instances of this new attack.

Jeff And in isolation, those one or two attacks just look like a member maybe forgetting their password.

Emily Or traveling out of state.

Jeff Yeah, the credit union is essentially fighting in the dark. By the time they realize a new tactic is being used across their system, the damage is already done.

Emily Which is why, Dr. Xie emphasizes that these institutions cannot fight this alone. Data Visor's approach to solving this data deficit is through what they call consortium signals and Industry Benchmark Knowledge consortium signals.

Jeff Okay.

Emily Yeah. Since a vendor like DataVisor works with a massive, broad set of customers banks, credit unions, payment providers, they have visibility into the global threat landscape.

Jeff Ah. So they pull the threat intelligence precisely. Like if someone spots a burglar checking door handles on one street, every single house in the zip code instantly upgrades their locks.

Emily That's a great analogy.

Jeff They take the attack patterns. They spot hitting a massive bank on the east coast and bake that domain knowledge into the tech stack, protecting a small credit union in the Midwest.

Emily It completely levels the playing field. The midsize institution benefits from a vast network of threat intelligence without having to gather all that data themselves.

Jeff Or suffer all those initial losses themselves.

Emily Right, exactly.

Jeff But if the defense is pulling its knowledge to create this global neighborhood watch, the attackers aren't just sitting still either.

Emily Not at all.

Jeff . The sheer speed of these real time networks means manual hacking is essentially obsolete. We are in a full blown AI arms race.

Emily We really are.

Jeff Dr. Xie specifically mentions that fraudsters are adopting highly sophisticated AI models like Mythos, which are designed to discover and share system vulnerabilities at terrifying speeds.

Emily Yeah, Mythos is a huge problem.

Jeff So how does an AI model actually discover a vulnerability in a bank's system? Like in practice?

Emily Well, instead of a human hacker manually typing passwords into a bank's login portal, they unleash an AI model to interact directly with the bank's back end architecture. The AI can simultaneously ping thousands of a bank's application programming interfaces. The API endpoints, which.

Jeff Are basically the back end doors that allow different software systems to talk to each other.

Emily Right? And the model brute forces these endpoints, altering its approach microsecond by microsecond, just looking for a single misconfigured line of code or a weak authentication check.

Jeff Oh, wow. And once it finds that tiny crack in the armor, it doesn't just exploit it once.

Emily No, it shares that specific vulnerability across illicit fraud networks instantly.

Jeff So if the bad guys are automating the attack at that scale, the good guys clearly can't rely on humans to write new rules to stop them.

Emily What's fascinating here is this is where Dr. Xie notes the critical shift from supervised machine learning to unsupervised machine learning.

Jeff Okay. I want to make sure we define the difference clearly for everyone.

Emily So traditional AI or supervised machine learning relies entirely on historical training data. Right.

Jeff Exactly. You feed the system ten million examples of fraudulent transactions and ten million examples of legitimate ones, and it learns the difference.

Emily But supervised learning has a massive blind spot. Because when fraudsters invent a completely novel scam that shares zero characteristics with past data, the supervised AI misses it entirely because it doesn't fit the historical label.

Jeff Right. That is the fatal flaw of supervised models.

Emily So how does unsupervised machine learning fix that?

Jeff Well, unsupervised machine learning does not rely on historical labels at all. Instead of looking for what it already knows is bad. It analyzes the raw, real time data streams and looks for hidden mathematical structures or correlations or behavioral anomalies.

Emily It's mapping out the subtle connections.

Jeff Exactly. It clusters data points together to identify things that are behaving synchronously or abnormally, even if it has no idea what the ultimate goal of that behavior is.

Jeff It flags the anomaly, even if it doesn't have a name for it yet. And according to the interview, this is crucial for detecting what Dr. Xie calls sleeper cells.

Emily Yes, sleeper cells are a huge threat right now.

Jeff And just to clarify, a sleeper cell in this context isn't an attack. It's a fake account created by a fraudster that looks entirely legitimate during the onboarding process.

Emily Right. The fraudster might even make a few small, normal transactions over several months to build up a history of trust. They age the account, basically.

Jeff So they're playing the long game.

Emily Exactly. The goal is to bypass the initial security checks so that weeks or months later they can execute a catastrophic fraud event from an account the bank's legacy system thinks is a trusted long term member.

Jeff It's literally the digital equivalent of a sleeper agent.

Emily It really is. An unsupervised AI is the only way to spot them.

Jeff Because it can see the big picture.

Emily Yeah, it can look at millions of accounts and realize that fifty accounts created over the last month across different IP addresses all have microscopic similarities. Like what? Maybe it's how they navigate the user interface, or the exact millisecond cadence of how quickly they type, or even the bizarre sequence of their initial micro deposits.

Jeff Things a human would never notice.

Emily Right? The AI flags the sleeper cell and neutralizes it at step one during onboarding or login, long before the actual attack ever launches.

Jeff And stopping fraud at step one is suddenly the most urgent priority in banking right now, because the actual infrastructure of money is changing.

Emily Big time.

Jeff We talked about the speed of real time payments earlier, but the stakes are getting exponentially higher. The interview points out that new real time payments, or RTP, have significantly raised the thresholds for wire transfers.

Emily We aren't just talking about Venmo -ing a friend for pizza anymore, right? RTP is designed for massive movements of capital. We are talking about business to business, supply chain transactions, real estate closings, major institutional transfers, real money. The thresholds are moving into the millions.

Jeff So if a scammer successfully breaches an account and initiates a fraudulent transfer over an instant channel, with these newly raised thresholds, millions of dollars can vanish instantaneously. Yes, and it is entirely irreversible.

Emily Completely.

Jeff The fear surrounding this is so high that many credit unions right now will accept RTP transactions, meaning they allow money to flow in, but they outright refuse to send them.

Emily Yeah, they are essentially disabling the outbound lane of the highway, because the risk of a catastrophic loss is just too massive for their balance sheets to absorb.

Jeff Okay, let me play devil's advocate here for a second.

Emily Go for it.

Jeff If an institution simply turns off the send button for real time payments out of fear, aren't they breaking the very system they're trying to offer?

Emily Well, yeah.

Jeff Like how is refusing to participate a viable business strategy in twenty twenty six? Consumers want instant transfers. If my credit union won't let me close on a house instantly, I'm just going to move my money to a mega bank that will.

Emily Right? And it isn't a viable long term strategy. It's a temporary panic measure. Refusing to participate means irrelevance. But on the flip side, locking down the system with extreme friction ruins the consumer experience.

Emily Which.

Jeff Credit unions hate.

Emily Right.

Emily We all despise those irritating is this you text messages that freeze your card when you're just trying to buy a coffee in a different city or, you know, holding up a legitimate contractor payment for three days while a bank investigates.

Jeff Because you can't lock down millions of dollars in real time by treating every single customer like a criminal.

Emily Exactly. This is where highly accurate, real time AI decisioning becomes the only viable path forward for these institutions.

Emily So the AI takes the heat off.

Jeff The.

Emily Customer.

Emily Yeah. When an AI can accurately assess thousands of data points in milliseconds, the device ID, the behavioral biometrics, the location history, the consortium threat signals we talked about earlier, right. It doesn't have to guess. It acts as a silent bouncer. It knows with a high degree of certainty whether the person hitting send on a million dollar transfer is actually you, or an AI impersonation bot.

Jeff It prevents the false alarms and preserves the frictionless, member friendly experience that credit unions base their whole identity on. Yes, the consumer just sees their transaction go through instantly, completely unaware that a massive algorithmic battle just occurred in the background to verify their identity.

Emily It silently neutralizes the massive threats while keeping the everyday user experience completely smooth. But you know, that brings up the logistical hurdle we mentioned earlier.

Jeff Oh, this is the part of the interview that really stood out.

Jeff We know the multi-million dollar stakes and we know this incredible AI tech exists, right? But how does a local credit union running on a tight budget with a small team, actually operate a futuristic defense system like this?

Emily Sounds impossible.

Jeff Right? It does. In the past, operating these cutting edge platforms is required. A highly technical mindset. You need a data scientists. You needed engineers who can write SQL queries to pull the right data from the servers. People who understood programming to test new mitigations.

Emily Which completely prices out the midsize institutions. They cannot afford to hire a dedicated team of Silicon Valley data scientists just to monitor their transaction logs. Right? This is why Dr. Xie's team introduced conversational AI agents into their financial crime prevention platform. It is a low code or no code solution.

Jeff So what does this all mean? Can a non-technical employee essentially chat with their fraud software like it's just another coworker sitting at the next desk?

Emily That's exactly what it means. Let's say a fraud analyst at a small credit union notices a slight uptick in suspicious new accounts, right? Instead of needing to code a complex database query to investigate, they can literally just type or speak to the platform.

Jeff Which is normal.

Jeff Conversation.

Emily Yeah, they can ask in plain English. Show me all accounts opened in the last forty eight hours that shared device IDs with known fraudulent IP addresses in our consortium data.

Jeff And the AI does the heavy lifting, translating the plain English into database code, running the query and presenting the data back to the analyst.

Emily It goes even further than that. The analysts can then ask the conversational agent to identify the attack pattern and test mitigations. Yeah, they can ask the system if we applied a block to this specific behavioral cluster you just found how many legitimate customers would be impacted.

Jeff Okay. Hold on. I have to stop you there. As a consumer, the idea of a non-technical bank teller or a junior analyst using a chat bot to write code that governs the security of my life savings, it sets off major alarm bells.

Emily I get that.

Jeff . We've all seen AI hallucinate facts or write bad code. What happens if this system hallucinates a security protocol and accidentally locks out half the credit union's legitimate members?

Emily That is the exact concern, which is why these systems operate within strict guardrails. The conversational AI isn't given autonomous control to change the live production environment.

Jeff Oh thank goodness.

Emily Right. It operates in a sandbox. When the analyst asks it to test a mitigation, the AI runs a simulation against historical data.

Jeff Like a practice run.

Emily Exactly. It presents the results of that simulation to the human. It says if you deploy this rule, you will block fifty fraudulent accounts and zero legitimate accounts.

Jeff Okay, that's much better.

Emily The human analyst then reviews the logic and hits the final approval button. The AI is a co-pilot, not the captain.

Jeff It democratizes the technology without removing the human oversight.

Emily Exactly.

Jeff And the real world application of this is already happening. The interview points to true cooperative Bank in Canada.

Emily Yeah. Great example.

Jeff They are a credit union using this exact tech to monitor everything from initial onboarding to login to simple profile changes.

Emily And think about the efficiency gains here. By empowering laypeople with AI, it frees up the human employees.

Jeff So they aren't just staring at screens all day.

Emily Right? Staring at transaction logs for anomalies is something humans are frankly terrible at anyway. The staff can focus on what credit unions do best.

Jeff Which is getting back to human facing community tasks, building relationships, helping members navigate complex financial needs like mortgages or small business loans.

Emily The AI handles the massive data processing and the humans handle the empathy.

Jeff I love that.

Emily And if we connect this to the bigger picture, it's vital that this technology is democratized and easy to use because fraud is not just a banking problem. No.

Jeff It's everywhere.

Emily Dr. Xie points out that the same technology is being adopted across airlines, e-commerce platforms, and shipping logistics.

Jeff Right? Wherever the money moves, the bad actors follow.

Emily Every industry that processes transactions needs this level of real time protection, and empowering non-technical staff with conversational AI is really the only practical way to scale this kind of advanced defense across the entire economy.

Jeff So let's take a step back and look at the journey we've just been on. We started with the reality that the sheer convenience of instant payments has inadvertently created a hyper speed playground for AI powered scammers.

Emily Yeah.

Jeff Scary one. Midsize institutions and credit unions found themselves painted with a target on their backs. Lacking the mass of data pools and budgets of the megabanks. Right. But by pooling consortium data to act as a global neighborhood watch, and by utilizing unsupervised machine learning to hunt down sleeper cells before they strike, they are fighting back.

Emily And they are managing to do it without sacrificing their identity. By integrating conversational AI as a co-pilot, these smaller institutions can deploy sophisticated security while preserving the low friction community soul that their members rely on.

Jeff It really is an invisible war. So to you listening, the next time you hit send on an e-transfer or drop money into a friend's account for dinner, and you feel that sense of safety when it goes through instantly without a hitch.

Emily Yeah.

Jeff Remember that you aren't just experiencing good software design. you are actually experiencing the quiet victory of a massive real time AI battle that was fought and won in milliseconds right beneath the glass of your screen.

Emily And you know that battle is never truly over.

Jeff No it isn't.

Emily The most lingering thought I took away from Dr. Xie's interview was her worrying about the nature of this arms race. Staying static means falling behind instantly.

Jeff Because the bad guys never stop.

Emily Right? Fraudsters are sharing vulnerabilities the exact second they find them. It forces us to ask a really difficult question. If institutions have to endlessly evolve just to maintain their current level of safety, will there ever be a final security measure? Or are we permanently trapped in a Red Queen race where our very definition of what makes a system safe expires and has to be completely rewritten every single day?

Jeff It definitely changes how you look at that simple tap on your phone. Dropping a meme into a chat might be effortless, but guaranteeing that your money arrives safely in real time. That might just be the most complex, high speed game of chess on the planet.

Emily It really is something to think about the next time you casually hit send. Until then, keep an eye on your accounts. And thanks for taking this deep dive with us.

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.