

COOPERATIVE CREDIT UNION ASSOCIATION & ASSOCIATION OF VERMONT CREDIT UNIONS

*C-Suite Roundtable • New England*

# When the Biggest Banks Panic,

## What Does That Mean for You?

Meghan Sutherland | CEO, FiVerity



# I've Seen Both Sides.

*Here's what the big banks won't tell you — and what it means for credit unions.*

Wells Fargo  
/ Wachovia

JP Morgan

UBS

CEO, FiVerity

## **The cooperative model is both the constraint and the advantage.**

The governance structures that slow some decisions are the same ones that make your members trust you with something personal. You cannot have one without the other. The question is knowing which decisions need full governance — and which ones don't.

## **Their size is a liability in a fast-moving environment.**

When the landscape shifts overnight, JPMorgan takes 18 months to respond. Not because they lack resources — because their structure makes speed impossible. Your structure gives you something different. Use it deliberately.

## **The gap is decision velocity, not resources.**

What JP Morgan spent a decade building, you can deploy today. The tools are democratized. What isn't democratized is the judgment to know which decisions need the board and which ones need you to just decide. That distinction is C-suite work.

# May 5, 2026.

Jamie Dimon stood on a stage with Anthropic's CEO and said this:

*"The risks are very real. AI has made it worse — it's made it harder. The banks in total are rather well protected. That doesn't mean everything that banks rely on is that well protected."*

— Jamie Dimon, CEO JPMorgan Chase



## **Claude Mythos: ~300 vulnerabilities in Firefox alone**

Earlier models found ~20. The AI-assisted attack window just compressed from months to minutes.



## **Access locked to 12 companies — Project Glasswing**

JPMorgan and Goldman got access. Your credit union did not. Broad release would hand attackers a weapon.



## **China is 6–12 months behind. That is the window.**

Anthropic CEO Dario Amodei's words. The window to act collaboratively before adversaries catch up is now.

# What "Panic" Means for Your Credit Union

*JPMorgan spends \$15B a year on technology and Dimon is still worried. Here's why that matters to you.*

## The Infrastructure Problem

Dimon wasn't talking about JPMorgan's own systems when he said "not everything is well protected." He was talking about **shared infrastructure** — payment rails, clearinghouses, open-source software, third-party vendors.

That's the stack your credit union sits on top of. JPMorgan patches their own applications first. The infrastructure your members depend on gets patched last.

**Your institution doesn't need to be the direct target. You just need to share infrastructure with one that is.**



## Fraud Attack Surface Just Expanded

AI-discovered vulnerabilities don't stay defensive. What Mythos found to protect, adversaries are finding to attack. More holes = more fraud vectors into member accounts.



## Big Banks Protect Themselves First

JPMorgan patches their stack in "a year or so." Your credit union's shared infrastructure gets addressed on a much longer timeline — if at all.



## The Collaboration Window Is Narrow

Six to twelve months before adversaries reach parity. The institutions building shared intelligence networks now will be positioned. Those waiting won't.

# Your Member Is Now the Threat Perimeter.

*And that changes everything about what relationship-based banking means.*

## THE OLD PERIMETER

- Firewall at the institution edge
- Fraud = external bad actor
- Authentication = safety
- If the member authorized it, it's clean
- Investigate after the loss

## THE NEW PERIMETER

- ✓ The member's phone is the perimeter
- ✓ Fraud = social engineering at scale
- ✓ Authentication tells you nothing about manipulation
- ✓ The member initiated it — and was coached to
- ✓ Intervene in the moment or it's too late

# This Is What Relationship Banking Actually Looks Like Now.

*JP Morgan can't buy what you already have: the relationship, the history, the name people trust with something personal. That is not a consolation prize. It is the only fraud defense that works at the moment of attack.*



## You Know When Something Is Wrong

A member who wires money to an unfamiliar account after a phone call from "the IRS" — your frontline knows that's off. That judgment can't be algorithmized. It comes from relationship.



## The Trust Signal Is Already There

Your members gave you something JPMorgan's algorithm will never get: genuine behavioral baseline. You know what's normal for them. That signal is the fraud detection tool.



## Friction at the Right Moment

The intervention isn't the investigation after the loss. It's the branch manager who pauses the transaction and asks one question. Relationship gives you the standing to do that.



## Proximity Is an Advantage, Not a Consolation Prize

Large FIs manage relationships at scale and lose the signal in the noise. Your credit union knows its community. That knowledge is a strategic asset — if you treat it like one.

# The Problem Relationship Can't Solve Alone.

*Institutions acting alone will always lose to criminals acting as a network.*

*Your fraud team is good. But they're only as good as the data they can see. And right now, that data ends at your own front door.*



## 1% of the Threat Landscape

Your team learns from your fraud only. The other 99% is happening across institutions you've never spoken to — and have no mechanism to speak to.



## No Cross-Network Pattern Recognition

The fraud ring that hit three New England credit unions last week uses the same synthetic IDs, the same playbook. Without shared data, you have no idea until they're in your door.



## Every CU Reinvents the Wheel

Every institution re-investigates the same case. Files the same SAR. Loses the same money. While the fraud ring moves on to the next member-owned institution working alone.

# "We've Got It Covered" Is the Most Dangerous Idea Right Now

*Said by someone who hasn't looked. "I don't know" interrupts the stack before it becomes a crisis. The institutions that get hurt worst aren't the ones with the smallest budgets — they're the ones where leaders performed certainty they didn't have and built cultures where no one felt safe raising the real question.*

**That's a leadership problem.**

Which means it's a leadership opportunity.

**"I don't know" is three words.**

Learned before five. Then professional environments teach people to stop saying it. Stopping is the mistake — especially right now.

**The Gyges's Ring principle.**

What does someone do when no one is watching? In a lean institution with no layers to absorb the gaps, that ring already exists. What your team does when no one is checking is exactly who you are.

# What Credit Unions Can Do Differently — Starting Now.

*Five moves that turn the cooperative model into a competitive weapon.*

<b>01</b>	<b>Treat the member as the perimeter — operationally, not just philosophically.</b>	Train frontline staff to pause, question, and protect. The intervention is the branch manager asking one question before a wire goes out. Build the culture around it.
<b>02</b>	<b>Build shared intelligence across your peer network.</b>	The cooperative model is the answer to the data silo problem. You already believe in shared ownership. Apply it to fraud intelligence. Share what you see. Pool what you know.
<b>03</b>	<b>Close the friction gap — strategically, not indiscriminately.</b>	Friction at the right moment saves members. Friction everywhere destroys relationships. Identify high-risk patterns — large wire transfers to new payees after phone contact — and build smart intervention there.
<b>04</b>	<b>Use your relationship baseline as a fraud detection tool.</b>	You know your members. That behavioral baseline — what's normal, what's not — is the signal that JPMorgan's algorithm will never have. Systematize it. Train your team to use it.
<b>05</b>	<b>Know which decisions need governance and which ones need you to just decide.</b>	Board approval belongs on major platform decisions and strategic partnerships. It does not belong on training your frontline to pause suspicious wires. Conflating the two is how the window closes while you're scheduling a meeting. The cooperative structure is the asset. Don't let it become the excuse.

# The Operating Model That Puts It Together.

*Identity Trust Management — built for the way fraud actually works today.*

01

## Alert Aggregation & Case Management

Unify all alert sources. Eliminate the queue backlog. Get every investigator working from the same intelligence layer — across all fraud types, not just 314(b).

02

## Fraud Investigation & Collaboration

314(b) requests, SAR drafting, cross-institution case sharing in one platform. Investigations that took days take hours. Because you start from what the network already knows.

03

## Threat Intelligence & Prevention

The culmination of collaborative activity. Consortium-fed signals that let you stop fraud before it reaches your members. Built for institutions your size — not retrofitted from JPMorgan.

**You are not the smaller,  
slower version of JP  
Morgan.**

**You are something they can't become.**

---

Fast enough to move this quarter.  
Trusted enough that your member picks up the phone.  
Close enough to the community to know when something is wrong.

**Request an Impact Assessment**

fiverity.com | [msutherland@fiverity.com](mailto:msutherland@fiverity.com)

