The "996 BRO" Startup Culture That Lets Fraud Win

Inside the Fraud Squad | Post #3 | July 2026

I once worked for a CEO who sent a Slack message on a holiday morning wondering where everyone was.

It was 10 AM. It was a federal / company holiday. People felt the pull — that invisible pressure that doesn't come with a direct order but arrives as a question mark at the end of a message from someone who controls your livelihood.

Most people went in.

That CEO wasn't unusual. That culture wasn't unusual. It has a name now: 996. And it's metastasizing across Silicon Valley in ways that go far beyond overwork — into something with real, measurable consequences for financial crime, fraud, and the safety of your money.

What Is 996?

The term comes from China's tech industry: work 9 AM to 9 PM, six days a week, 72 hours of labor dressed up as ambition. The Chinese government tried to ban it. Workers there pushed back hard. It spread anyway, because the people setting the schedules weren't the ones working them.

Now it's crossed the Pacific. NPR reported last fall that the schedule is "capturing the interest of Silicon Valley leadership" — and the framing matters. *Leadership* interest. Not worker enthusiasm. The people celebrating 996 are, almost universally, the people not doing it.

As historian Margaret O'Mara put it, Silicon Valley has always had a "California casual exterior and a workaholic interior." The free food, the ping-pong tables, the climbing walls — all of it was designed to keep people at their desks longer. 996 is just the same idea with the pretense stripped away.

It skews young. It skews male. It eliminates anyone with caregiving obligations, health constraints, or the audacity to want a life outside the office. And it creates a particular kind of culture — one that rewards loyalty to the org over judgment, speed over diligence, and volume over quality.

That combination is where financial crime finds its opening.

The Compliance Officer in a 996 Shop

Here's what 996 BRO culture actually produces inside a fintech: a compliance function that is chronically understaffed, structurally underpowered, and culturally dismissed.

I've been a board-appointed BSA Officer at multiple fintech companies. I know what it feels like to walk into a leadership meeting and explain why you need to freeze accounts, file SARs, and slow down an onboarding flow — while everyone else in the room is being evaluated on how fast they can grow.

In a 996 shop, growth is the only religion. The BSA Officer is the person who keeps saying "no." The General Counsel is the person who finds a way to say "yes." The CEO is the person who sends Slack messages on holidays because the numbers need to hit.

In that environment, the message to compliance isn't always explicit. It doesn't have to be. It comes through in budget decisions, headcount approvals, and the unmistakable signal of which meetings you get invited to and which ones happen without you.

I've sat across from executives who told me, straight-faced, that my "approach to compliance was creating problems for everyone." That my account freezes were costing the company revenue. That certain things needed to move forward without my sign-off.

I didn't move forward. Not everyone has the professional standing to make that call. And fraud rings know it.

$200 Billion. That's What "Move Fast" Costs.

The PPP fraud disaster is the definitive case study in what happens when growth culture crushes compliance culture — and this time, it happened with taxpayer money.

When the pandemic hit in 2020, fintechs were given an extraordinary opportunity: process Paycheck Protection Program loans at scale, earn fees for doing it, and help small businesses survive an economic catastrophe. Some did it well. Many did not.

The SBA's own Inspector General found that at least $200 billion — roughly 17% of the $1.2 trillion disbursed — showed indicators of fraud. Two fintech startups alone, Blueacorn and Womply, processed one-third of all PPP loans in 2021. Congressional investigators found that up to nearly half of Blueacorn's loans and up to one-third of Womply's may have had fraud indicators. Together, they collected an estimated $2–4 billion in processing fees from taxpayers for doing it.

The House Select Subcommittee investigating the matter put it plainly: these companies may have "failed to adequately screen PPP loan applications for fraud," resulting in "millions of dollars worth of FinTech-facilitated PPP loans being made to fraudulent, non-existent, or otherwise ineligible businesses."

As recently as April 2026, the SBA referred 562,000 suspected fraudulent loans to the Department of Treasury for collections, totaling $22 billion — the largest referral package in SBA history. These were loans flagged for fraud years earlier and never collected on.

That number — $22 billion — isn't the result of sophisticated criminal masterminds outsmarting the system. It's the result of a system that was designed, under pressure, to move fast and ask questions later. Or never.

"The agency weakened or removed the controls necessary to prevent fraudsters from easily gaining access to these programs," the Inspector General report concluded. "The allure of 'easy money' in this pay and chase environment attracted an overwhelming number of fraudsters."

Pay and chase. Approve now, investigate later. That's 996 BRO compliance in its purest form.

The Pattern Doesn't Change

The PPP disaster was the largest single fraud event in fintech history. But the pattern — growth pressure eliminating compliance friction, creating a window that criminal networks immediately exploit — is not unique to 2020.

I've watched it happen at scale in crypto onboarding. In neobank account opening. In peer-to-peer payment networks. In stablecoin corridors. The actors change. The infrastructure changes. The underlying dynamic does not.

Fraud rings don't break your defenses. They wait for you to remove them yourself — and 996 BRO culture is one of the most reliable mechanisms for that removal. Not through malice, usually. Through the slow accumulation of small decisions: the compliance hire that gets postponed, the review queue that gets accelerated, the SAR threshold that gets quietly adjusted, the BSA Officer who gets excluded from the product roadmap meetings.

Each decision seems reasonable in isolation. Together, they open a door.

The Character I Keep Writing

In *Scurry (Fraud Squad)*, the protagonist spends a lot of time in those meetings. He knows the pattern. He's seen it in Kandahar and in conference rooms. He knows that the moment an executive starts framing compliance as a cost center, the institution is already losing the war.

He doesn't always win the argument. Nobody does, in the short run. The win comes later, when the regulators show up, or the DOJ calls, or the OIG report drops, and the executives who were so confident about moving fast are nowhere to be found.

The fraud squad doesn't get credit for the fights it wins before anyone notices there was a fight. That's the job.

996 BRO culture creates a world where that job becomes nearly impossible — and where $200 billion can disappear into a compliance blind spot while everyone's busy celebrating their growth metrics.

The invisible war is real. And culture is the front line.

Eric Kinney is a Certified Fraud Examiner, former BSA Officer, and DOJ witness. He is the CEO and Co-Founder of Scurry, and the author of Scurry (Fraud Squad), now available on Amazon. New posts in the Inside the Fraud Squad series publish twice monthly at erickinney.com.

Follow: @scurryfraudsquad on Instagram | LinkedIn