BioCatch | Report

2025 GLOBAL SCAMS

Using behavioral and device intelligence to shine a light on social engineering scams

October 2025

About this report

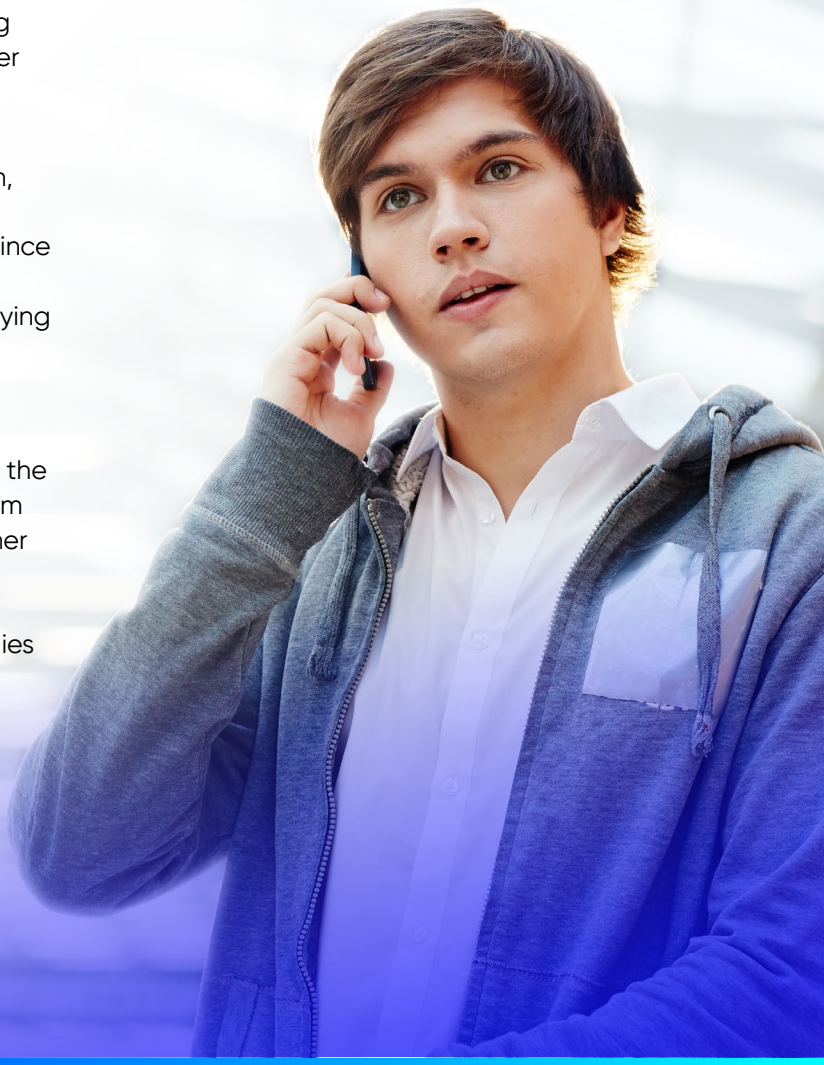
The origins of authorized push payment (APP) fraud — more commonly known and henceforth referred to as "scams" — probably date back to the infamous Nigerian prince emails we all received in the 1990s. But scams as a fraud type didn't begin its ascension to the worldwide scourge it is today (wreaking more than $1 trillion and counting in losses every year, as the most costly and prevalent form of fraud globally), until the 2008 launch of Faster Payments in the U.K. Real-time payment systems drastically improved the effectiveness of scams by all but closing the window of time during which victims could reverse their mistakes.

More recent improvements in bank defenses against unauthorized fraud gave scams another bump, as fraudsters pivoted from hacking into accounts to instead manipulating account holders into willingly granting them access. Finally, as it has every industry, GenAI has supercharged scamming (which is now very definitely an industry), lowering the barrier to entry and helping scammers scale and improve their attacks all over the world.

At its core, every scam relies on psychological manipulation, trickery, and so-called social engineering. Scammers intentionally deceive their victims, spinning yarns that convince legitimate accountholders to transfer their funds away to strangers — in the name of love, investment, commerce, paying one's debts, employment, familial responsibility, and more.

The following report analyzes scam data from financial institutions serving nearly 350 million consumers on five different continents. As we'll explore in the following pages, the global scam problem is only getting worse, with overall scam attempts increasing exponentially, every year, in every corner of the world. Scams are running rampant and undetected past traditional fraud defenses, making the investment in and deployment of new defensive and offensive technologies more vital than ever before.

At its core, every scam relies on psychological manipulation, trickery, and so-called social engineering.



Scams by the numbers

65%
increase in the total number of scams reported by BioCatch customers between 2024 and 2025

14%
year-over-year increase in purchase scams, which remain the most prevalent scam type in the world

100%
spike in voice phishing (vishing) scams, making vishing the second-most-reported scam type

10x
surge in smishing (phishing that utilizes SMS texts instead of emails)

63%
uptick in romance scams

42%
increase in investment scams

15%
decrease in impersonation scams

Regional focus on scams

Scam trends in the U.S. and Canada

Since 2023, reported scams in the U.S. and Canada have more than quadrupled, underscoring an urgent need for continued vigilance and awareness among both consumers and institutions.

Three scam types stand out:

- Purchase scams: Fraudsters trick people into paying for goods or services that never arrive or don't exist. These scams account for nearly half of all cases in the region by volume.
- Impersonation scams: Criminals pose as trusted individuals or organizations to steal money or personal information. Reported cases dropped year over year, in part due to increased controls by banks leveraging our technology.
- Vishing scams: Scammers use phone calls to pressure victims into sharing sensitive information. Reports have increased by a factor of 15, though volumes remain lower than other more common scam types.

Many scams go unclassified, often because of insufficient information. That gap can stem from weak follow-up processes or the absence of reimbursement rules. Still, our customer data shows a 16% decrease in unclassified scams, suggesting banks are improving their reporting practices.

Scam trends across Europe

In the past 12 months, reported scams in Europe have nearly doubled, underscoring the growing threat that scams pose to consumers and financial institutions across the continent.

In our analysis of customer data, we identified four key insights:

- Romance scams — schemes in which fraudsters build fake online relationships to gain victims' trust and exploit them financially — have doubled every year since 2023, marking one of the biggest changes.
- Voice scams, in which fraudsters trick victims using social engineering (typically impersonating a bank or law enforcement), have also doubled. This method has proven effective, though banks, particularly in the U.K., are controlling losses using advanced detection tools such as behavioral intelligence.
- False online purchases account for one in four scams.
- Job scams account for less than 1% of all cases but are rising sharply, with volumes quadrupling in the past twelve months.

In Europe, the share of scam payments directed to new beneficiaries is lower than in any other region — a trend some in the industry attribute to tools like Confirmation of Payee in the U.K., which requires name verification when payments go to new recipients. In theory, this makes it harder for scammers to deceive their victims, though in practice fraudsters often find ways to explain away name mismatches.

Regional focus on scams

Scam trends in Latin America

Scam volumes in Latin America have surged over the past year, increasing by a factor of six. The sharp increase is likely tied to three factors: 1.) more scam attempts by fraudsters, 2.) greater awareness by banks and victims driving higher reporting, and 3.) improved fraud management processes that give banks more intelligence on scams.

Unfortunately, despite improved reporting numbers, the vast majority of these scams are unclassified, making it difficult to understand which scam types are most common. That said, our data shows smishing — text message scams that lure victims into clicking malicious links or sharing personal details — has increased by a factor of 14, while vishing — phone-based scams where fraudsters pressure victims into revealing sensitive information — has tripled.

Scam trends in Asia-Pacific

In the Asia-Pacific (APAC) region, scam volumes rose by 35% over the past year, marking a significant increase. The trend, however, varies by region. In Australia, data shows a decrease in scam losses, while the Indian subcontinent and Southeast Asia show a rise in reported scams.

In our analysis of the data, we've identified the following key insights:

- Romance scams and investment scams — which prey on trust, affection, or the promise of high returns from fraudulent opportunities — both doubled in volume across the past year. These scam types rely heavily on exploiting human emotions.
- Impersonation scams, typically involving vishing, are the most reported scams across the region. Bank reports show a 25% rise in cases from last year. This trend appears elsewhere across the globe and likely reflects the success fraudsters have experienced with this scam type, particularly the bank impersonation variety.
- Purchase scams are on also the rise, though less pronounced than other scam types.

Inside the industrialization of fraud

Erin West | founder, Operation Shamrock

In February, I traveled 1,000 miles across Cambodia. I didn't encounter a mere handful of back-alley, pop-up scam camps in the country. I found entire cities transformed into penal colonies for fraud: massive, college-campus-sized compounds built to hold thousands of trafficked workers forced to conduct online scams, day and night.

What's unfolding in Cambodia is more than a crime wave. It's the industrialization of fraud — human trafficking fused with organized crime, protected by power and scaled to the size of cities. Scam compounds have turned parts of the country into hubs of forced labor that defraud people worldwide. And as the model spreads across Southeast Asia and beyond, Cambodia's experience ought to serve as a warning for how far this industry can spread if left unchecked.

A look inside

In the coastal city of Sihanoukville, the transformation is shocking. Once a beach town, the scam metropolis remains lined with towering hotels. But there are no tourists inside. Every building is filled with workers whose passports have been seized and freedoms stripped. Bars cage the windows, laundry hangs from every floor, cell towers sit on rooftops, and guards lock down every gate. From a distance, it looks like development. Up close, it's a prison.

On the road to the city of Chrey Thom, the pattern repeats. Rows of seven- and eight-story compounds rise from what used to be a quiet border town, now covered in barbed wire, steel gates, and armed guards. Some compounds are still under construction, while others are already packed. It has the feel of a boomtown, but instead of producing goods, the entire industry is fraud.

Walking up to one compound, the facade appeared almost ordinary — a fence, a sign, a gate. But the second we lingered, guards appeared. These were men in uniforms, outfitted in tactical gear. And they wanted us gone. It was clear: These are not apartment complexes. They are fraud factories, operating openly and with protection from people in power.

Lives bought, freedoms stripped

Inside, the workers are treated as commodities. I am in contact with human-trafficked victims, both presently inside the compounds and those returned home, who tell me they were bought and sold for thousands of dollars — $3,000, $5,000, even $16,000 a head. If workers try to escape, they are beaten or resold to another compound. Their so-called job is to spend every waking hour defrauding strangers online. There is no way out.

What I found most disturbing was how normal it all looks from the street. Right next to these compounds are restaurants, clothing shops, and even a new boardwalk along the river. Joggers run by, families sit on benches, a man walks his dog. Ordinary life continues just yards from places where thousands are imprisoned. The scamming isn't hidden anymore. It's integrated into the community.

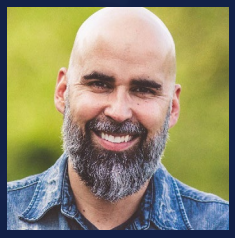
Cambodia represents organized crime on a transnational and industrial scale. This isn't a backroom operation or something happening in the shadows. Entire cities are now dedicated to scams, operating openly, protected, and expanding.

Beyond Cambodia

Cambodia is only the beginning. The same model is spreading across Southeast Asia and beyond. It is visible in Myanmar's border towns, Laos's special economic zones, parts of the Philippines, and across borders in Africa and South America.

The U.S. Department of State's **2025 Trafficking in Persons Report** underscores that this pattern is no longer confined to one region — it's part of a global surge in human trafficking tied to organized online crime. The report warns that weak governance, corruption, and high digital profits are creating ideal conditions for expansion.

What started in Sihanoukville is now a blueprint being copied wherever governance is weak and profits are high. These are not isolated incidents. They are evidence that the model works. And the world is full of places where this could happen next.



A fight for humanity

Ian Mitchell | founder, The Knoble

I've been fighting fraud for around 26 years now. I used to think the worst problem I faced was a new data breach or missing my financial plan because of an identity theft ring hitting our bank. But my blinders are off, and many across the industry are coming to the same realization: The financial system is being exploited to exploit people.

These crimes take many forms: generational wealth stolen through scams, people enslaved in scam centers, images of exploited children bought and sold online, money moved across the world to fund other heinous crimes. The reality is that organized criminal activity is not only stealing money. In some cases, it's also stealing lives.

The financial services industry is in a unique position to fight for good. Financially motivated crimes infiltrate every part of the system, utilizing online, mobile, in-person, gift cards, cash, and every other channel and payment method imaginable.

By my estimate, more than 660,000 people around the world wake up each day to fight financially motivated crimes. These professionals already have the best data, technology, and processes in place to monitor suspicious activity and take action. And now more than ever, both awareness and substantive actions are accelerating. The sleeping giant of the financial industry is waking up. This industry will use all of its tools and influence to snuff out the criminals exploiting the integrity of our financial system.

Whether motivated by financial security, reputation, or simply by the drive to do what is right, the financial sector will win this war, because it must. If you work in the financial sector — whether as an investigator, data analyst, or manager — you have the opportunity to get involved, to do good, and to protect people.

Be bold. Bank with heart.

Case study

Scams are not only a growing financial threat. They also carry a devastating human cost. Behind every fraudulent transaction is a victim whose trust, savings, and peace of mind have been compromised.

Every scam has a human cost.

BioCatch data shows a 65% increase in reported scams between 2024 and 2025, underscoring the scale and urgency of the problem. But the numbers tell only part of the story. Victims are often manipulated into making decisions that, from the outside, seem unthinkable, draining accounts, taking on new debt, and even concealing the truth from loved ones.

To highlight this all-too-common scenario, we're sharing a case study from a real BioCatch banking customer in Europe. It shows how a seemingly ordinary set of transactions can reveal the devastating hold a scammer can have over someone's life. In this case, a mother undergoing cancer treatment entrusted her daughter with her banking credentials, creating an opening for exploitation. The story shows how fraudsters prey on vulnerability, how behavioral data can expose who's really behind an account's activity, and why recognizing these patterns is critical to protecting people from both the financial and emotional toll of scams.

View the **full case study here**.

BioCatch | Report

About BioCatch

BioCatch prevents financial crime by recognizing patterns in human behavior, continuously collecting more than 3,000 anonymized data points – keystroke and mouse activity, touch screen behavior, physical device attributes, and more – as people interact with their digital banking platforms. With these inputs, BioCatch's machine-learning models reveal patterns in user behavior and provide device intelligence that, together, distinguish the criminal from the legitimate. The company's Customer Innovation Board – an industry-led initiative in partnership with American Express, Barclays, Citi Ventures, HSBC, National Australia Bank, and others – collaborates to pioneer innovative ways of leveraging customer relationships for improved fraud detection. Today, more than 30 of the world's largest 100 banks and 287 total financial institutions deploy BioCatch solutions, analyzing 16 billion user sessions per month and protecting more than 532 million people on more than 1.6 billion devices around the world from fraud and financial crime.

www.biocatch.com E: info@biocatch.com @biocatch in /company/biocatch