
Financial crime
Detection
WHAT HOLDS BANKS BACK?
RedFlag
Accelerator
by RedCompass Labs

Contents

Foreword

There's nothing organized crime wants more than for us to continue doing what we're doing.

$3.1 trillion in illegal transactions were made in 2023. More than $800 billion was connected to drug trafficking, $350 billion to human trafficking, and $11.5 billion to terrorism. Another $500 billion was lost to fraud.

1% of these crimes are brought to justice. That feels like an error of focus. Not an error of ability.

It's easy to become cynical, but that doesn't solve the problem. It's easy to feel overwhelmed, underfunded and over regulated, but that doesn't solve the problem either.

Whether laundering money from fentanyl, people, weapons, or abusive images of children, organized crime is banking on us to continue doing exactly what we're doing now.

Human beings alone cannot solve financial crime. We need data. Whether it's transaction data, banking data, external data, public source data, open-source data, or dark web data. You need all of it. And you need to know what you're looking for to put it into context. That includes the latest up-to-date red flags, models, and personas.

You will need curious, autonomous AI agents that know what they are looking for and never tire or get distracted. AI agents that can build cases by drawing on previous investigations and serve them up to humans to make decisions.

We need to be looking for today's fraud and money laundering methods, not those from years or even months ago.

That is the recipe. We need to know the flags specific to the crime and the persona, so you can ask the right questions; the right data from the open and dark web; and systems that process this both conventionally and support AI.

"Am I seeing a human trafficking victim? A perpetrator? A money launderer cleaning the proceeds of drugs and people smuggling? What am I seeing?"

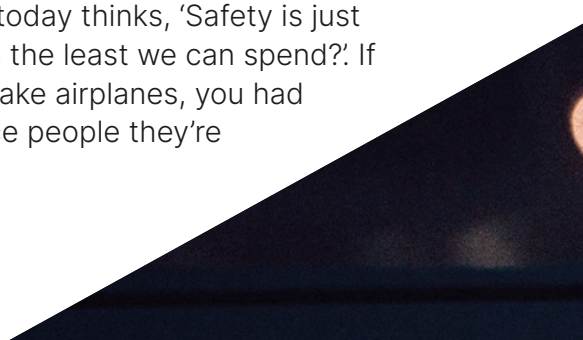
Today, there's enough intelligence, enough data, powerful AI and new technology to have a 10X solution. We could solve and find 10 times the amount of dirty money flowing through our payments channels, banks and accounts.

What stops us? Well, it's us, right?

Institutional inertia waiting for a regulatory push. Treacle from wasted, unproductive meetings. Fear of new technology and data sharing. Money.

Organized crime is banking on our inability to adapt as fast as they do.

No car maker today thinks, 'Safety is just a cost: what is the least we can spend?'. If you want to make airplanes, you had better convince people they're



> “**You will need curious, autonomous AI agents** that know what they are looking for and never tire or get distracted”

safe. Restaurants that are unhygienic are shut down no matter the quality of food. Why do we accept a 1% detection rate?

Once scams start hitting home – and they will – people and companies will move their money to safety. So, stopping scams means retaining deposits.

If we make fraud and money laundering harder, we make the buying and selling people and images of children harder, too

It’s not that the problem is so hard and so complex. It’s that we hide behind process and data-sharing interpretations. It is underfunding the teams that want to do more. It is when AML vendors underfund their platforms. It’s us, right?

But we can change that.

We have the technology, the open-source data, the dark web data, and the ability to understand who is transacting, whether through IP addresses or multiple personas. We have the flags, the AI, and the tools. We have the recipe to double or triple crime detection, to 10X it.

The question is, do we have the will?

I think we do – I hope we do.
This is our watch. **This is our lawn.**

Tom Hewson,
CEO, RedCompass Labs

Introduction

In 2021, US consumers lost $1.7 billion to investment fraud.
In 2023, they lost $4.6 billion.

The human trafficking industry generated $150 billion in 2014. In 2024, it is thought to exceed $350 billion. Drug trafficking was worth $652 billion in 2013. Estimates now exceed $800 billion.

Whatever way you cut it, however much we think is being done, however much progress we feel we are making, financial crime is on the rise and getting more complicated.

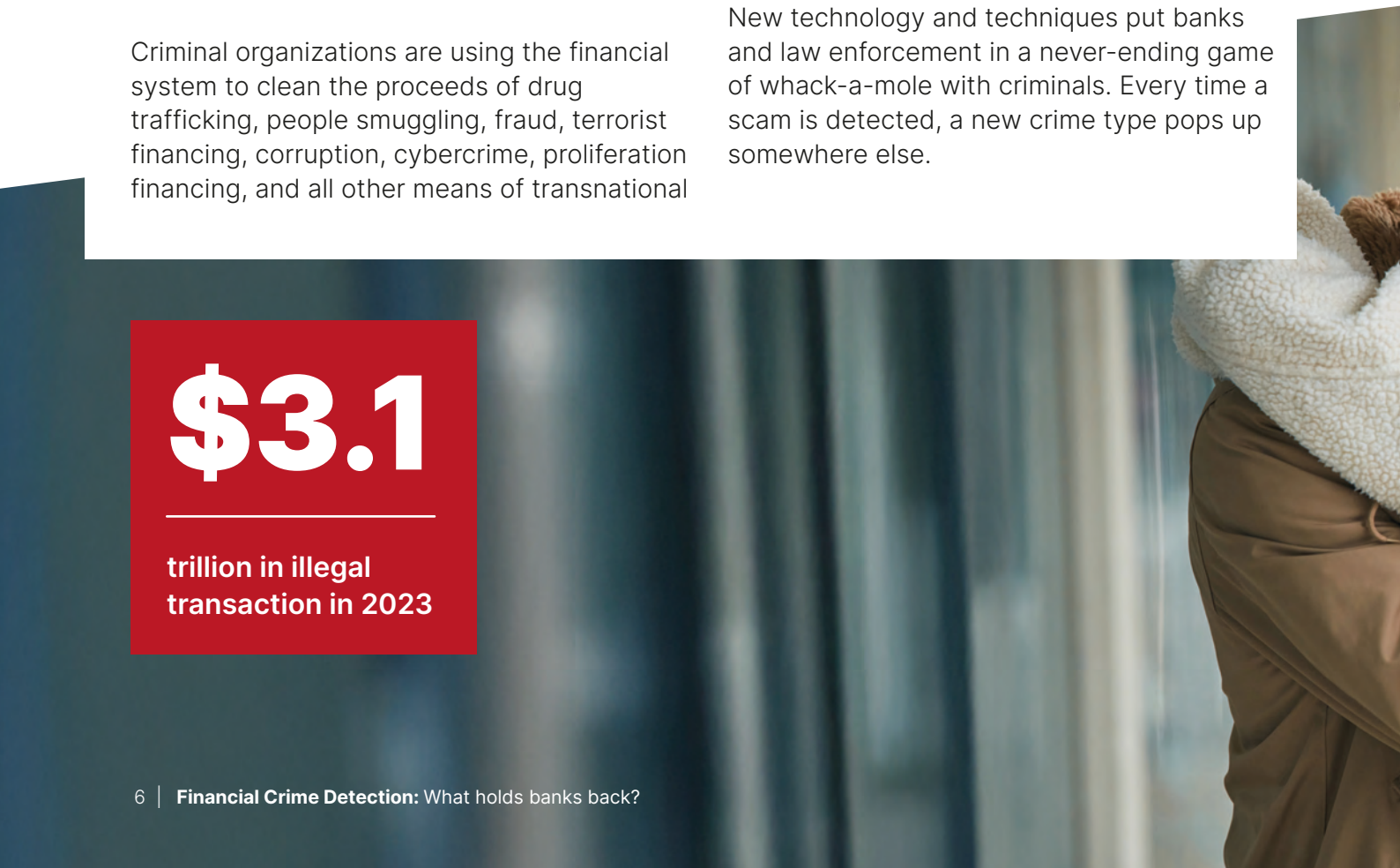
$3.1 trillion of illicit funds flowed through the financial system in 2023. Our most generous estimates suggest we can only find 10% of the money laundered by international criminal gangs. The more sobering and perhaps realistic statistic often quoted is that just 1% of financial crimes are ever brought to justice.

Criminal organizations are using the financial system to clean the proceeds of drug trafficking, people smuggling, fraud, terrorist financing, corruption, cybercrime, proliferation financing, and all other means of transnational criminal operations. The proceeds flow freely from the gangs to an international web of money mules into financial institutions.

Bank deposits are structured across multiple accounts and money service bureaus and fall just under the threshold for investigation. The money trickles in undetected.

The gangs use AI and deep fakes to prey upon the elderly and unsuspecting. Fake online profiles extort our children from afar while gift cards and cryptocurrency disguise the flow of funds. Vulnerable people are trafficked for work and sex in businesses that outwardly claim to offer legitimate services. Shell companies disguise ownership.

New technology and techniques put banks and law enforcement in a never-ending game of whack-a-mole with criminals. Every time a scam is detected, a new crime type pops up somewhere else.



$3.1

trillion in illegal transaction in 2023

A turning tide

As unwitting facilitators, payment service providers (PSPs) are under increasing pressure to take greater responsibility for financial crime.

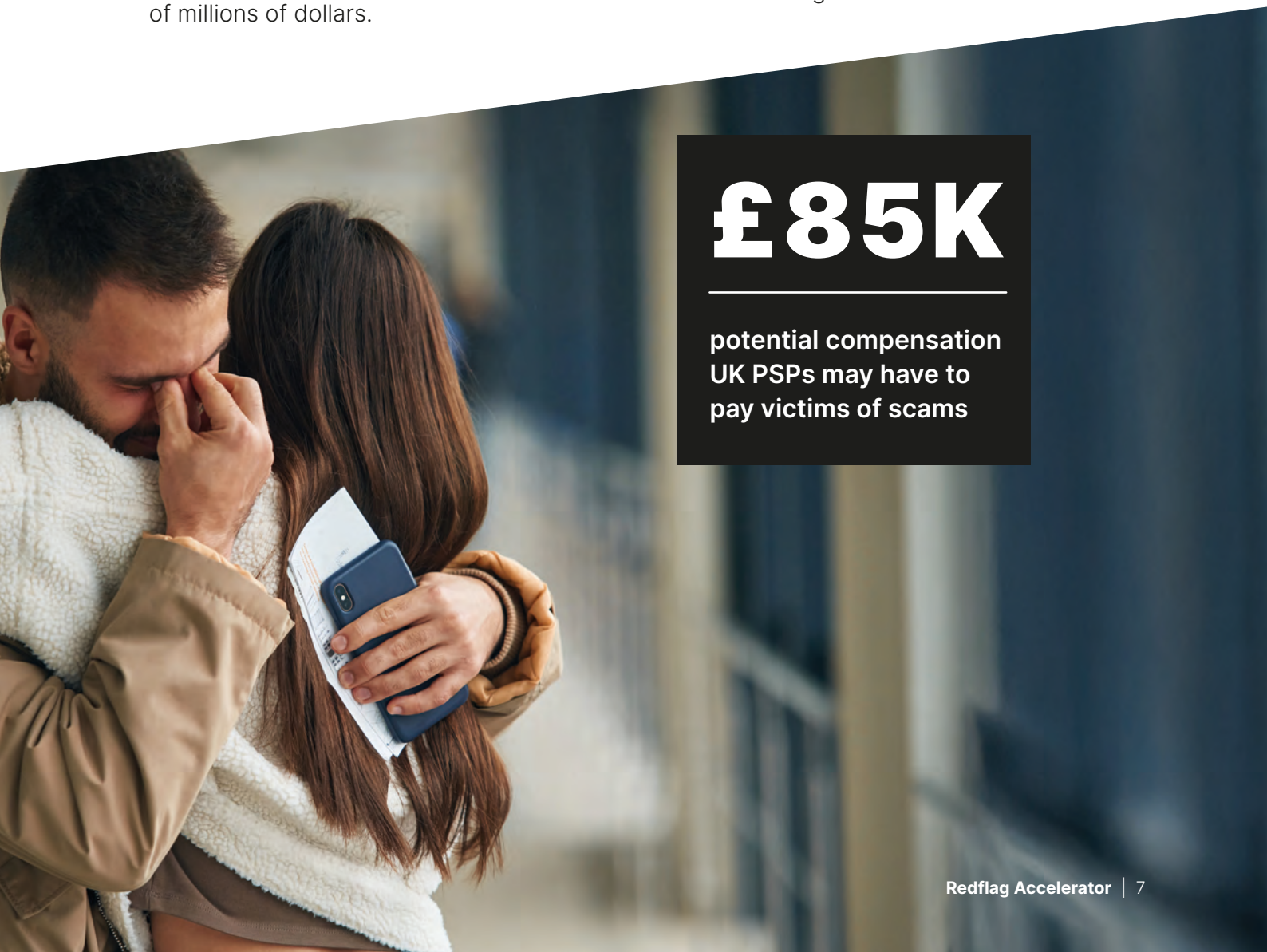
In October 2024, for example, UK PSPs may be required to reimburse victims up to £85,000 per transaction if they have been scammed.

If the UK's new rules are successful, global regulators may follow suit. Banks may soon find themselves legally responsible for customer fraud loss to the tune of hundreds of millions of dollars.

There are no mandatory reimbursements in the US or Canada as it stands. But banks will reimburse victims to avoid bad press, reputational damage, and legal scrutiny. (See: US banks reimbursing victims scammed on Zelle, the bank-owned person-to-person payment service.)

As soon as businesses and consumers feel a bank will not protect, support, or reimburse them, fair or unfair, their money will move to banks that will.

Banks are certainly commercially bound to act. Soon they could be legally bound. The tide is turning.



£85K

potential compensation UK PSPs may have to pay victims of scams

The survey

In 2021, the Financial Crimes Enforcement Network (FinCEN) identified eight national Anti-money Laundering (AML) and Countering the Financing of Terrorism (CFT) priorities that underscore the evolving nature of financial crime:

1/ Corruption

The misuse of power by government officials for illegitimate private gain.

2/ Cybercrime

Criminal activities conducted online, including hacking, data breaches, and the theft of financial information.

3/ Terrorist financing

The funding of terrorist activities, which can involve complex financial networks and illicit transactions.

4/ Fraud

Includes a wide range of deceptive practices to secure financial gain, including identity theft, phishing, romance scams, investment scams and more.

5/ Transnational criminal organization activity

Involves criminal organizations that operate across borders, engaging in activities like drug trafficking, human smuggling, and money laundering.

6/ Drug trafficking

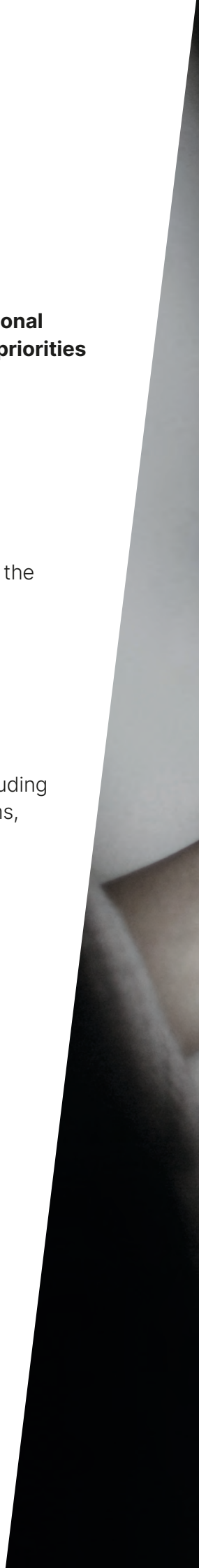
The illegal production, distribution, and sale of drugs, often linked to organized crime.

7/ Human trafficking and smuggling

The exploitation of individuals through force, fraud, or coercion for purposes such as forced labor or sexual exploitation.

8/ Proliferation financing

Refers to the funding of the spread of weapons of mass destruction and their delivery systems.



These crime represent a mix of new and long-standing threats to the US financial system and national security.

With these priorities in mind, we surveyed 300 senior payments professionals at US banks to better understand how financial services are addressing the multi-trillion dollar epidemic that is financial crime. More specifically, we wanted to understand what is holding us back from detecting more than 1%.

We use the FinCEN priorities to explore the challenges banks face in identifying and combatting the most difficult crimes, the strain on resources, and the approaches big and small banks are taking to invest in fraud prevention and anti-money laundering (AML) efforts. Perhaps most importantly, we look at the impact of new technology and reveal gaps in banks' responses to the rapidly changing criminal landscape.

Here's what we found.

The rise of ‘pig butchering’ scams and human trafficking

Some of the most prevalent scams today were unheard of just a few years ago. Take ‘pig butchering’ as an example.

This uniquely terrible crime dupes vulnerable people into making fake cryptocurrency investments. The victims are tricked into thinking their investments are doing well, and that they should invest more to get bigger returns (this is known as ‘fattening the pig’). When it comes to withdrawing the money, the scammers disappear, leaving the victims penniless.

What makes this crime so uniquely terrible is that the scammers are often victims of human trafficking themselves. Many are recruited under the false promise of legitimate work, only to find themselves enslaved. They have quotas to hit. If they don’t meet their targets – if they don’t exploit other people – they are beaten, raped, some even have their organs harvested.

According to the FBI, victims reported losses of nearly 4 billion from pig butchering scams and other crypto fraud in the US last year—more than double the previous year. The true scale, however, is unknown.

With this in mind, we asked banks which specific crimes they are currently prioritizing for prevention. They were presented with a comprehensive, though not exhaustive, list of crimes that are either on the rise or have reached concerning levels.

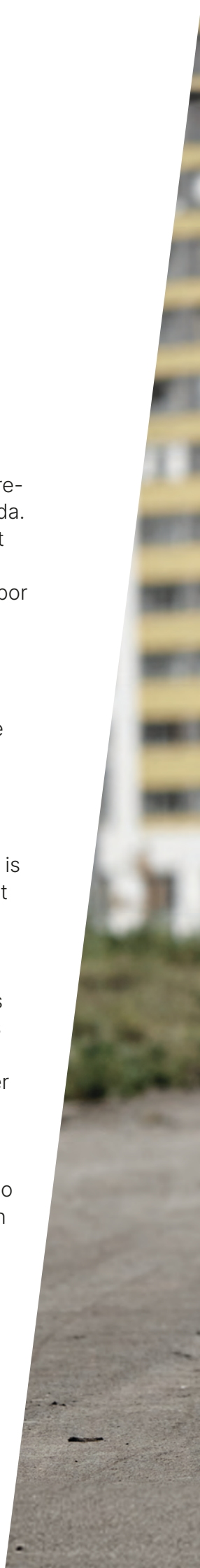
Our research shows human trafficking-related crimes are top of the banks’ agenda. Commercial-front brothels featured first (31%), closely followed by efforts to combat people smuggling (30%) and labor trafficking (30%).

Larger banks show a stronger focus on labor trafficking (39%) and elder abuse (39%), while smaller banks appear more focused on emerging threats like pig butchering scams (41%).

Interestingly, and rather strikingly, pig butchering (a new and emerging crime) is on par with drug trafficking (a persistent and pervasive crime).

Sextortion, another new, devastating crime impacting teenage boys, receives less attention. Just over a fifth of banks (22%) rate it as a key concern. That’s despite a tenfold increase in the number of cases since 2021 and more than a dozen related deaths. A recent case involved the extradition of two Nigerian men to the US to face charges related to online extortion and their involvement in the suicide of a Michigan teenager.

It’s clear that banks have a battle on their hands.



COMMERCIAL - FRONT BROTHELS

30.9%

Sex traffickers use legitimate businesses to exploit people for sex services. Restaurants, bars, nail salons, bars, and clubs of all types are used to house the abuse.

LABOR TRAFFICKING

29.9%

Victims are forced to work, often in manual jobs, under threats, coercion, or deception. They live in squalor with little or no pay, their passports are stolen, and they're cut off from the outside world.

DRUG TRAFFICKING

28.2%

The cultivation, manufacture, distribution, and sale of substances that are subject to drug prohibition laws.

ROMANCE SCAMS

25.3%

Fraudsters create fake online personas to build romantic relationships with victims, eventually deceiving them into sending money or personal information.

SEXTORTION

21.6%

A form of online blackmail. Criminal gangs create fake online profiles to trick their victims, often teenage boys, into sending nude images and videos. The gangs threaten to share the images with the victim's friends and family if they do not pay.

PEOPLE SMUGGLING

30.2%

Vulnerable people are transported across borders, usually in exchange for money, often under dangerous conditions, and without documentation or legal status.

ELDER ABUSE

28.6%

Elderly people are susceptible to a wide range of scams. They're seen as more trusting and are often less used to technology. Shockingly, carers and family members are the most common abusers.

PIG BUTCHERING

27.2%

A unique and modern threat which gets its name from fattening pugs before slaughter. Victims are tricked into fake cryptocurrency investments. Sadly, the abusers are often victims of human trafficking themselves.

ONLINE CHILD SEXUAL EXPLOITATION

23.9%

Children are graphically abused for money, often by their parents. The consumers are often white males from Australia, the US and the UK.

The top five hardest crimes to detect

Financial crime is hard to detect, but certain crimes are harder to spot than others.

We asked banks which of the FinCEN priorities banks find the most difficult to find and why. We found a poor understanding of the personas involved, and internal governance are major reasons:

33%

1. PROLIFERATION FINANCING

Proliferation financing refers to the provision of funds or financial services to aggressive and destabilizing 'proliferation actors. These actors may use the funds to obtain materials, components, data, technologies and expertise to enhance their capability to develop chemical, biological, radiological and nuclear (CBRN) weapons.

Complex and concealed networks, front companies, shell entities, plus the fact that many of the goods involved have both civilian and military applications, make it difficult to spot.

WHAT MAKES IT SO HARD FOR BANKS TO DETECT?

24.49% / IT system release slots

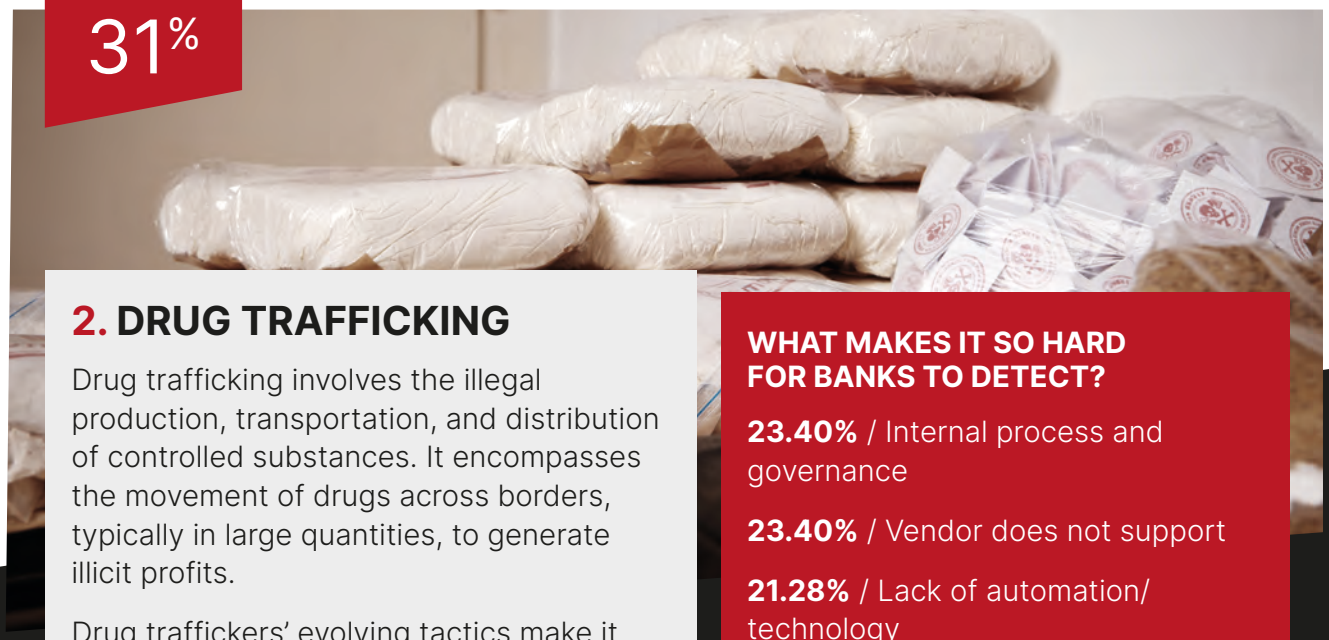
23.47% / Internal process and governance

22.45% / Latest model information

22.45% / My vendor does not support

21.43% / Poor understanding of the personas involved (including victims, offenders, facilitators, money mules)

31%



2. DRUG TRAFFICKING

Drug trafficking involves the illegal production, transportation, and distribution of controlled substances. It encompasses the movement of drugs across borders, typically in large quantities, to generate illicit profits.

Drug traffickers' evolving tactics make it difficult for banks to identify these illegal transactions effectively. Traffickers often use shell companies, cash-intensive businesses, money mules and sophisticated money laundering techniques to disguise their activities.

WHAT MAKES IT SO HARD FOR BANKS TO DETECT?

23.40% / Internal process and governance

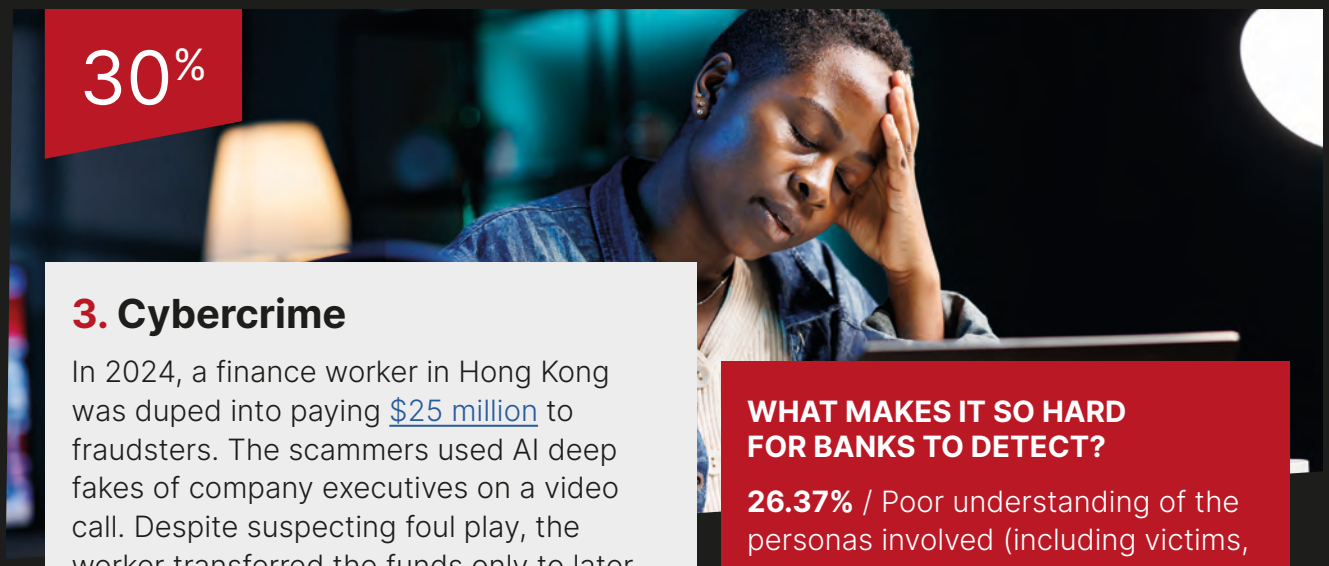
23.40% / Vendor does not support

21.28% / Lack of automation/ technology

20.21% / Testing

20.21% / Poor understanding of the personas involved (including victims, offenders, facilitators, money mules)

30%



3. Cybercrime

In 2024, a finance worker in Hong Kong was duped into paying $25 million to fraudsters. The scammers used AI deep fakes of company executives on a video call. Despite suspecting foul play, the worker transferred the funds only to later realize his mistake.

It's no surprise, then, that cybercrime scored high. New technologies, such as AI, are making cybercrime much harder to detect and prevent. Criminals are sophisticated, highly motivated and move quickly. Banks must work hard to match their pace.

WHAT MAKES IT SO HARD FOR BANKS TO DETECT?

26.37% / Poor understanding of the personas involved (including victims, offenders, facilitators, money mules)

26.37% / IT system release slots

21.98% / Lack of automation/ technology

21.98% / Latest model information

21.98% / My vendor does not support

29%

4. HUMAN TRAFFICKING AND HUMAN SMUGGLING

We often think of slavery in historical terms, but we shouldn't. There are an estimated 50 million people trapped in modern slavery today –more than the populations of Norway, Sweden, Denmark, Finland, Iceland and the Netherlands combined. More than at any other point in human history.

People are bought and sold into work and sex and forced to live in squalor. They're coerced, threatened, beaten and cut off from the outside world. The traffickers work hard to hide their activities. Commercial-front brothels, seasonal farm work, and overseas construction companies mask the abuse. But banks can spot clues in financial data. They just need to know what to look for.

WHAT MAKES IT SO HARD FOR BANKS TO DETECT?

25.58% / Latest model information

25.58% / IT system release slots

23.26% / My vendor does not support

20.93%/ Internal process and governance

20.93%/ Poor collaboration (between bank-to-bank, bank-to-law enforcement, and law enforcement-to-bank)

29%

5. DOMESTIC AND INTERNATIONAL TERRORIST FINANCING

Terrorist financing remains a critical threat, with international groups like ISIS, Al Qaeda, Hizballah, Hamas and Iran's IRGC relying on funding through banks, money services, and digital assets. These funds support recruitment, logistics, and attacks. Domestically, anti-government extremists and domestic violent extremists (DVEs) pose significant threats and often use low-cost financing tactics. Financial institutions can prevent financing by complying with sanctions, maintaining robust AML programs, and reporting suspicious activity to disrupt terrorist networks.

WHAT MAKES IT SO HARD FOR BANKS TO DETECT?

26.37% / Poor understanding of the personas involved (including victims, offenders, facilitators, money mules)

26.37% / IT system release slots

21.98% / Lack of automation/ technology

21.98% / Latest model information

21.98% / My vendor does not support

Banks' resources are stretched across a multitude of financial crimes

How do banks prioritize their resources across the FinCEN priorities?
Are some categories more important than others?

To find out, we asked bankers how they split their time and budgets across the FinCEN priorities. Our data reveals a fairly even split.

'Terrorist financing' and 'other fraud (including account takeovers and check fraud)' demand marginally more time and budget than other crimes (12%). Meanwhile, corruption receives the least attention (10%).

Authorized-push-payment (APP) fraud – a hot topic, particularly with the rise of instant payments – holds a mid-level spot in both lists (11%). Yet interestingly, smaller banks devote significantly more time (17%) and budget (17%) to APP fraud.

With limited resources spread across various fronts, financial institutions must continually refine their strategies to address both emerging threats and persistent challenges effectively.

TIME

CATEGORY	PERCENTAGE
Corruption	9.66%
Cybercrime	10.61%
Domestic and international terrorist financing	11.32%
Authorized-push-payment fraud	10.74%
Other fraud (account takeover, check fraud, etc.)	11.76%
Transnational criminal organizations	10.14%
Drug trafficking organizations	10.80%
Human trafficking and human smuggling	11.08%
Proliferation financing	10.52%
Other	3.37%

BUDGET

CATEGORY	PERCENTAGE
Corruption	9.73%
Cybercrime	10.86%
Domestic and international terrorist financing	11.17%
Authorized-push-payment fraud	10.83%
Other fraud (account takeover, check fraud, etc.)	11.67%
Transnational criminal organizations	10.30%
Drug trafficking organizations	10.41%
Human trafficking and human smuggling	10.45%
Proliferation financing	11.15%
Other	3.43%

Banks take too long to update fraud models

Banks need to move at least as fast as criminals to maintain current detection levels, and they need to move even faster to have an impact.

However, our data suggests a significant portion (59%) take between four and six months to update their fraud models after identifying new red flags for money laundering or other financial crimes. That means they take longer than the criminals to adapt.

In an ideal world, banks would update their fraud models daily to stay on top of emerging crime types. Yet we found nearly every bank (99%) does not.

What's interesting is that most of these issues stem from internal inefficiencies. Banks are burdened by bureaucracy; it's the banks getting in their own way.

50 million people are enslaved today. Men, women and children are forced to have sex and work against their will. Their passports are stolen. They're cut off from the outside world. They're beaten, raped and killed. And we can only find 1% of these crimes, in part, because internal governance gets in the way.

We can do more. Banks must recognize the urgency of these issues and find a way to update their models daily with the latest red flags.

What prevents banks from updating their fraud models daily and the results were as follows:

27%	Internal governance
26%	Too complicated
24%	Not a priority
24%	Change process
23%	Latest model information
22%	Testing
22%	Budget
22%	My vendor does not support it
22%	IT system release slots
17%	Not enough staff

59%

of banks take 4 – 6 months to update their fraud models

Are banks using the latest tech better than criminals?

The race to leverage the latest technology is like a never-ending game of whack-a-mole.

Banks must guess where criminals might try and maneuver next. Most (94%) banks believe they are very good at using the latest technology, and nearly half (49%) strongly affirm this belief.

The confidence is particularly pronounced among larger banks, where every respondent believes they are effectively leveraging technology such as AI.

Yet when asked if criminals are proficient at using the latest technology, fewer banks agreed. Nine in ten (91%) acknowledge that criminals are adept at using modern technologies for financial crime, but only four in ten (41%) strongly agree. Just eight in ten (82%) large institutions agree that criminals are proficient in using the latest technologies to commit financial crimes.

While banks recognize the evolving threat, they maintain a belief that they are superior when it comes to the latest tech. This confidence may be misplaced.

8 in 10

large institutions agree that criminals are proficient in using the latest technologies

Banks are *(at least)* eight months behind criminals

The financial sector is facing a sobering reality.

Despite considerable investments in technology and an estimated $17.3 billion spent on fraud detection and prevention solutions in 2024, banks believe they are trailing behind criminals by an average of 8.2 months.

A deeper dive into the data reveals varying perceptions among banks of different sizes. For instance, a quarter (26%) of smaller banks estimate that criminals are just 2-3 months ahead.

However, some larger institutions fear that the gap could be as wide as 23 months.

A small but significant number (4%) of banks believe that criminals are 2-3 years ahead in their use of technology, while a smidgen (1%) believe the gap could be as wide as 4-5 years.

We know criminals are adopting and adapting to new technologies faster than many banks anticipate. We know it takes banks more than 4 months to update their fraud models. And now we know that banks think criminals are eight months ahead. How optimistic are the banks?

Banks think they can catch up

Despite an eight-month head start and detection rates as low as 1%, banks say that they can catch up.

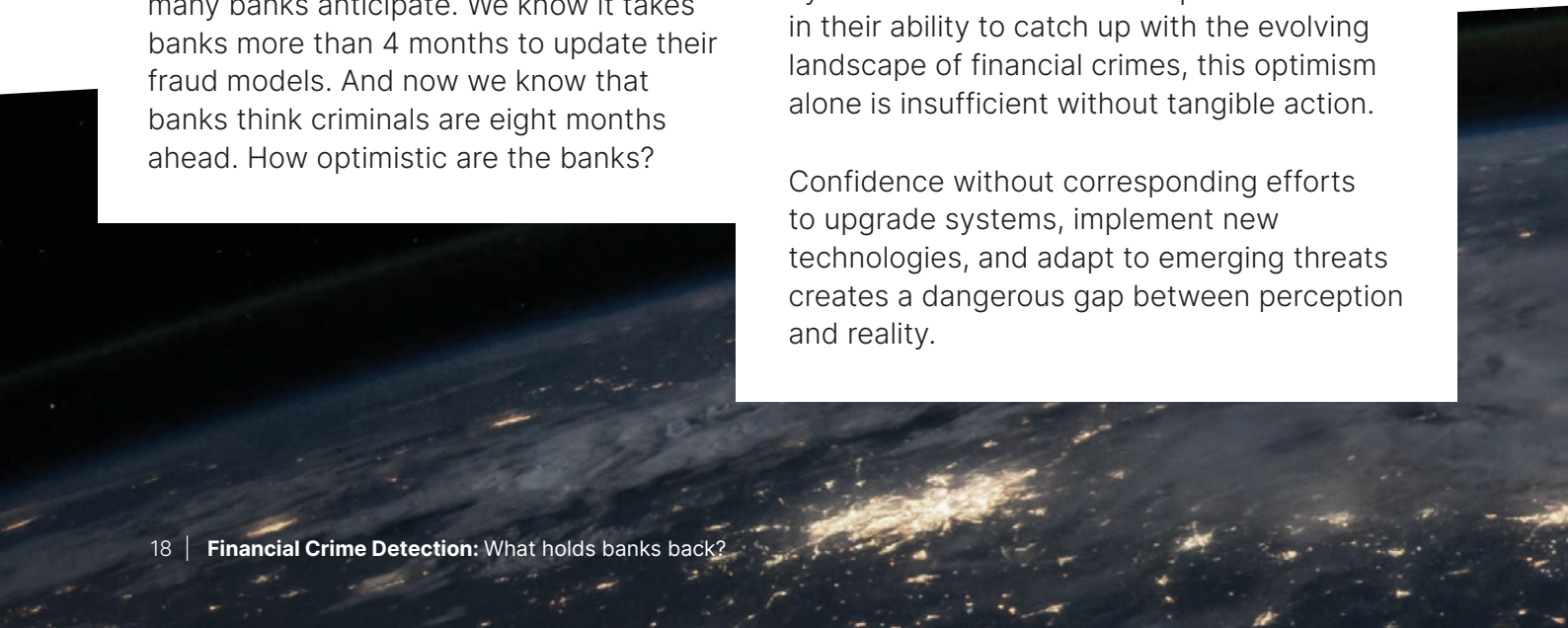
Three-quarters (75%) believe they can successfully close this gap, while a quarter (25%) express cautious optimism, feeling that they "maybe" could catch up. None of the banks surveyed expressed doubt in their ability to eventually match or surpass criminals' technological capabilities.

Small banks are slightly less optimistic than big banks. Eight in ten (81%) showed confidence in their abilities to keep pace with or outpace the criminal. while every large institution expressed confidence. Nearly six in ten (57%) big banks are "very confident" in their ability to tackle these challenges.

Banks also feel well-prepared to address emerging technological threats such as AI and deep fakes. A substantial nine in ten (90%) report feeling ready to confront these challenges. Four in ten (41%) express a high level of confidence.

Larger banks are even more confident. Nearly six in ten (57%) stated they are very confident in their readiness to tackle these new forms of cyber threats.While banks express confidence in their ability to catch up with the evolving landscape of financial crimes, this optimism alone is insufficient without tangible action.

Confidence without corresponding efforts to upgrade systems, implement new technologies, and adapt to emerging threats creates a dangerous gap between perception and reality.



How banks believe they can close the gap

Banks recognize a multi-faceted approach is needed to catch up with the criminal networks:

39%

1 / The implementation of new technology

Banks plan to invest in advanced cybersecurity tools, artificial intelligence, and machine learning systems that can detect and respond to threats in real-time. By embracing cutting-edge technologies, banks aim to match and exceed the capabilities of criminal networks.

39%

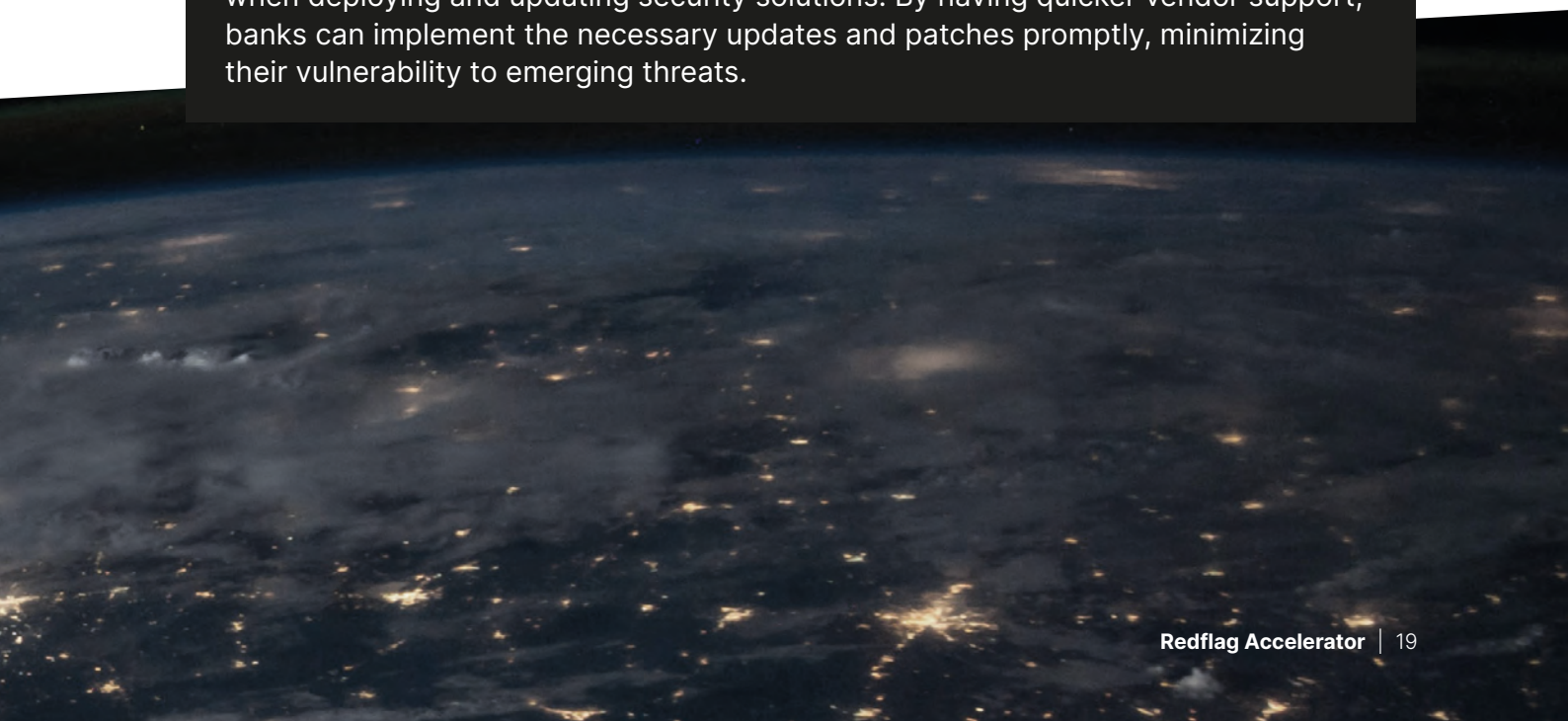
2 / Streamlining internal processes

Banks understand that efficiency is key to staying ahead of cybercriminals and are prioritizing streamlining internal processes, automating routine tasks and improving communication and coordination across departments. By optimizing these processes, banks can respond to threats more quickly and effectively, ensuring that their defense mechanisms are agile and robust.

38%

3 / Faster vendor support

Banks need faster and more responsive support from their vendors, especially when deploying and updating security solutions. By having quicker vendor support, banks can implement the necessary updates and patches promptly, minimizing their vulnerability to emerging threats.



Is AI a help or a hindrance? Banks are divided

As AI continues to revolutionize the world, its role in financial crime remains a subject of intense debate.

Some view AI as a powerful tool that could potentially eradicate financial crime. Others fear it may complicate detection efforts by making it easier for criminals to operate undetected.

We asked banks what they thought, and a significant portion are wary of AI's impact on financial crime detection. More than half (57%) believe that AI will make it more difficult to detect financial crimes. Some (16%) fear AI may render detection nearly impossible.

Conversely, just under a third (31%) of banks believe that AI will ease the detection of financial crimes, with less than one in ten (7%) expressing the bold belief that AI could eventually eradicate financial crime.

Bigger banks are more optimistic about AI's potential. The majority (54%) think AI will simplify detection, while more than a third (36%) believe AI could eliminate financial crime altogether. This optimism likely stems from access to greater resources and the ability to invest in cutting-edge AI technologies and talent.

AI is great at detecting good and bad payments in the transaction process, but the payments industry has not yet come to terms with a paradigm shift in which bank accounts and merchant websites are taken over by fraudsters.

It's no longer a question of whether a transaction is fraudulent – now it's a question of who owns a legitimate bank or merchant account, and where funds are coming from.

16%

of banks fear AI may render detection nearly impossible

36%

of banks believe AI could eliminate financial crime altogether

Shifting from rules to personas: a new approach to financial crime prevention

Most banks use a rules-based typology to find suspicious payments, which looks at transactions in isolation.

However, this kind of monitoring is too noisy. In a typical rules-based financial investigation unit, over 95% of alerts are classified as false positives. Even when a match is genuine, the actual risk is often far from clear. But if we take a persona-based approach that explores behaviors in context with external reference data, things become clearer.

Consider Sunset Spa, a hypothetical Beauty Salon in the US. Sunset Spa's details have been found on several commercial sex advertising sites. A quick look at their transaction history shows they're making regular payments to these websites.

There doesn't seem to be much payroll expenditure, which is unusual for a beauty salon, particularly one that's making as much money as Sunset Spa. Plus, they seem to be making regular purchases at drug, fast food, and sex stores.

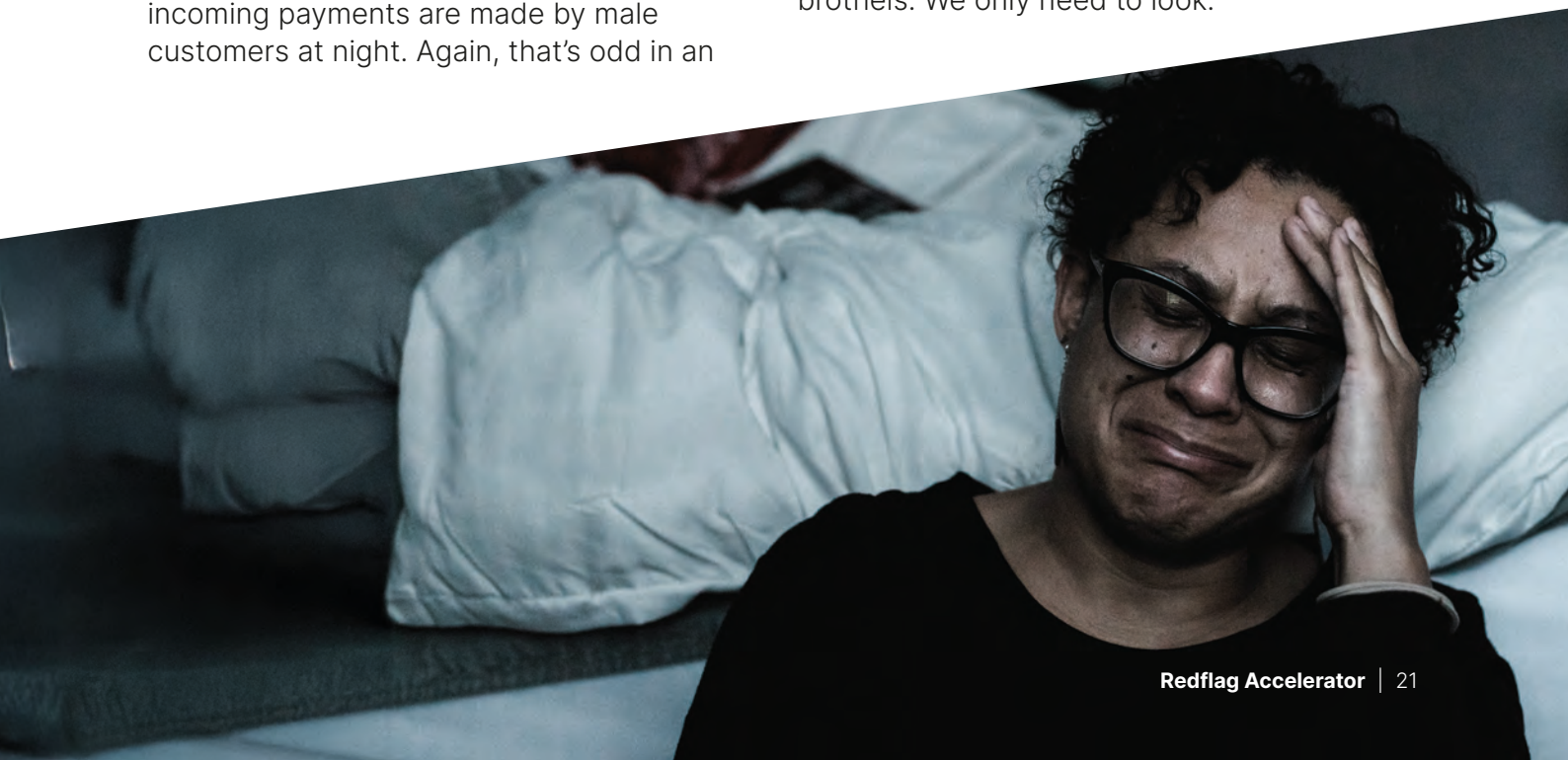
On closer inspection, we find that most incoming payments are made by male customers at night. Again, that's odd in an industry with a mostly female clientele that operates in daytime hours. None of this fits the usual profile for a beauty business.

With the current rules-based approach to anti-money laundering, much of this goes undetected. (The majority of commercial-front brothels are discovered after tip-offs from locals.)

But with the right reference data, red flags, and persona-based approach, we can start to ask the right questions.

Why isn't Sunset Spa spending anything on payroll? Why are their details showing up on websites advertising sex services? Isn't it strange that most of their clients are men? And why are so many of them getting a massage at 2 am?

It doesn't take much digging to uncover what's hidden behind commercial-front brothels. We only need to look.



Conclusion

Financial crime is a multi-trillion-dollar epidemic. Whichever way you cut it, it's growing and it's getting harder to detect.

New technology, techniques, and scrutiny are placing more pressure on banks than ever before. The rise of pig butchering and the pervasiveness of human trafficking highlight the need for new strategies. Yet banks' resources are stretched across multiple fronts, with small teams and meager investment. It takes banks longer to update their fraud models than it does for criminals to adapt.

Why? Our research suggests it could be the banks themselves: internal governance, a lack of understanding of the personas involved. But these are easily solved.

Out of every person on this planet, every 1 in 185 is in slavery. Think of all the people you pass on your way to work. 1 out of 185 is huge.

If we don't have the money, the resources, or the will to save the equivalent of the whole of Scandinavia and The Netherlands from slavery, if we cannot save children from online sexual abuse or vulnerable people from their life savings, we have to wonder why that is.

1 in 185

people on the planet are in slavery

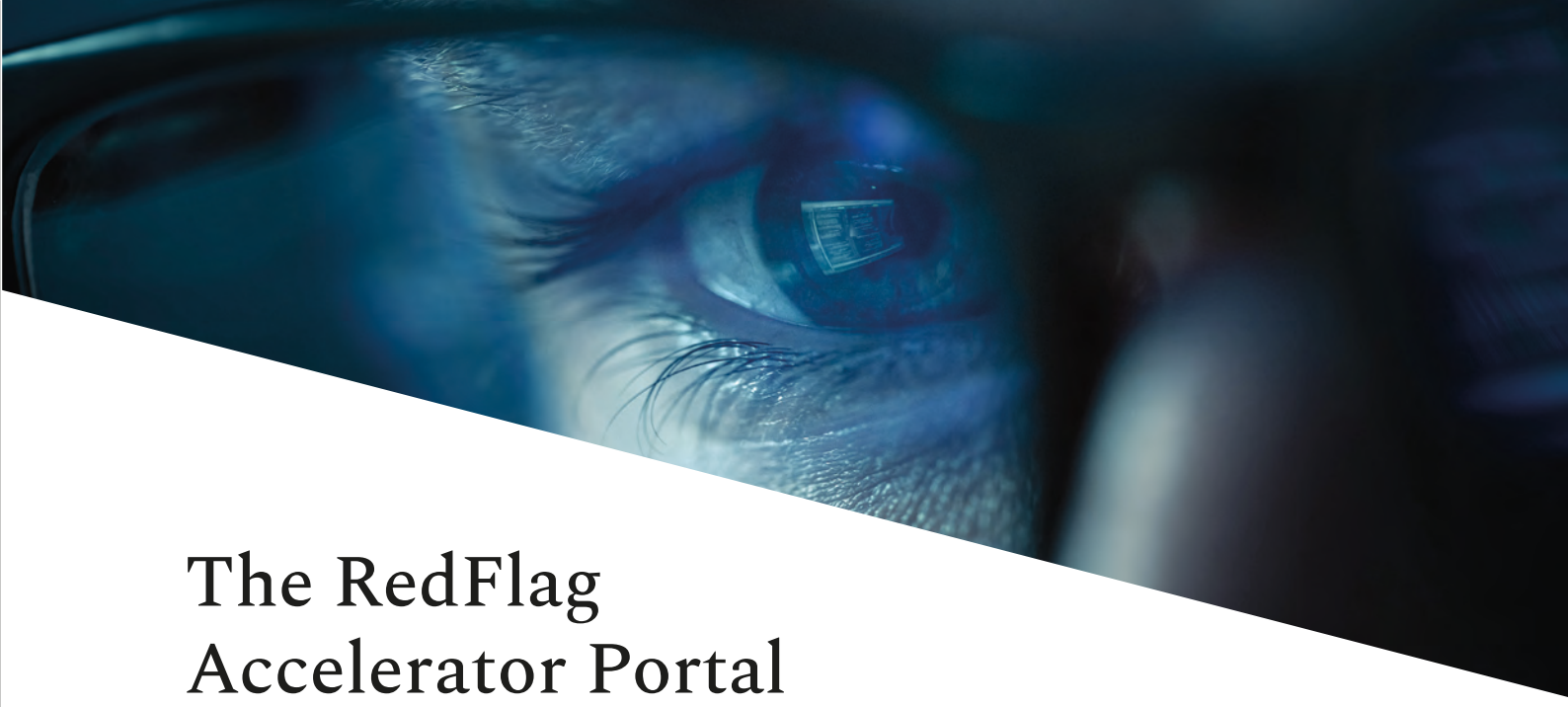
Banks, by their own admission, are 8 months behind the criminals. They know the criminals are good at using the latest technology, yet they rate themselves marginally better. This confidence may be misplaced. Only 1% of financial crimes are brought to justice. How can these two things be true? How can it be that banks are very good at using technology to combat financial crime, and yet 99% goes undetected?

The good news is that banks are confident they can catch up, and they know that technology is the key ingredient.

With the right reference data, red flags and a persona-based approach, we can tell from ATM transactions when someone appears to be moving brothel or sex workers from town to town. We can look at various purchases, deposits and parts of the data and we can follow it on a map. We can tell when a farm worker is being paid a proper salary, and we know when that salary is being removed because the farm is employing a slave. We can see it in the data. It takes the right technology and tools. We can find it if we want to.

For human trafficking to go from $150 billion to $350 billion in six years shows that the criminals are entrepreneurial, innovative, and on the cutting edge of technology. They must not be underestimated.

We need a new way of detecting financial crime. Fortunately, it exists.



The RedFlag Accelerator Portal

The RedFlag Accelerator is the world's most comprehensive database of persona drivers red flags that enables banks and financial institutions to close the gap by speeding up the discovery of financial crimes with gold-standard actionable intelligence and data. It not only facilitates expertise sharing across financial institutions but it also efficiently and reliably allows any bank to keep up with the continuous changes in global financial crime.

RedCompass Labs AI

RedCompass Labs AI tools work alongside and inside AML vendor platforms and bank data solutions. We can help to monitor, investigate and update humans on the latest models and suspicious activity, enabling you to make meaningful decisions to stop financial crime on their platforms

About RedCompass Labs

We believe that there are only two types of payments – good and bad. We enable good ones; We help stop the bad.

We exist to help open the doors of finance to all, and to protect those who enter.

We are experts in instant payments, faster payments and frictionless payments. Whether domestic or cross border, we have been working with ISO 20022 for 15 years, and as payments move faster, we have been on the leading edge of implementing these schemes all around the world.

RedCompass Labs is a source for world-class payments experts, as well as microservice-based toolkits that accelerate payment platform builds, updates, and scheme adherence. Our technology reduces the need for complex payment platform customizations, increases platform functionality, and decreases project risk.

As payments accelerate, their use for causing harm multiplies. The RedCompass Labs RedFlag Accelerator is the gold standard of red flags for providers of payment services. We use these flags and a persona-oriented approach to provide investigation tools and algorithms that identify human crimes such as labor and sex trafficking, child sexual exploitation, elderly abuse, and fraud, occurring in payment providers' data. We provide AML (Anti Money Laundering), Sanction and Fraud system integration, upgrades and tuning, using data analytics tools we have developed.

We support our clients from offices in the UK (London), Poland (Warsaw), North America (Miami, Toronto), Belgium (Antwerp), Japan (Tokyo) and Singapore.

We do payments. We accelerate the good - instant, faster, frictionless, real time, and cross-border payments. We help stop the bad - human crimes, labor and sex trafficking, sanction lists, and fraud. That is who we are.

THE REDFLAG ACCELERATOR PORTAL

Exposing financial crime with gold-standard actionable intelligence and data.

www.redflagaccelerator.com

RedFlag Accelerator
by RedCompass Labs