A FREE FIELD GUIDE · FINANCIAL CRIME ADVISORY

THE FRAUD PLAYBOOK

25 Years of Financial Crime — How It Evolved, and How to Stop It.

FOR AUSTRALIAN BUSINESSES THAT MOVE MONEY

FINANCIAL CRIME ADVISORY

Contents

1. **Part 1 — How Fraud Evolved:** 25 Years on the Front Line
2. **Part 2 — The Modern Fraud Taxonomy:** Every Threat Operating Today
3. **Part 3 — How to Stop It:** A Defender's Playbook
4. **Part 4 — Sector Playbooks:** Where the Money Moves
5. **What to Do Next:** A 90-Day Action Plan
6. **A Note on the Future**
7. **About Financial Crime Advisory**

01

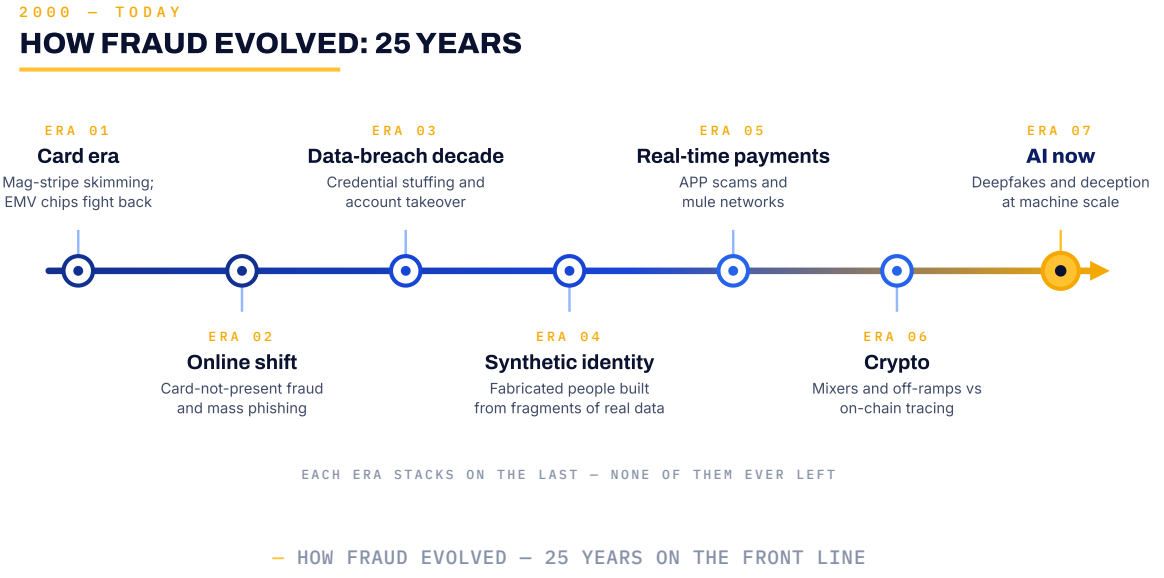
Part 1: How Fraud Evolved — 25 Years on the Front Line

Fraud is not a fixed problem. It is an adversary.

That single idea is the most important thing in this book, so we will start with it. A pothole does not learn. A flood does not read your incident report and change tactics next quarter. Fraud does. Behind every scheme is a person, or increasingly a small industry of people, watching where the money moves, where it moves fastest, and where nobody is looking closely. They test your defences for free, at scale, every single day, and they only need to be right often enough to make a living.

Over twenty-five years the tools have changed almost beyond recognition — from a strip of magnetic tape to a synthetic voice that sounds like your CFO — but the underlying behaviour has not. Fraud follows two things: the money and the technology. When the money speeds up, fraud speeds up. When a new technology creates a gap between "convenient" and "verified," fraud lives in that gap until someone closes it. Then it moves.

What follows is a history of that migration. Not a museum tour — a map of an arms race, told in the eras I have watched it pass through, because the pattern of how each era ended tells you almost everything about how to fight the one we are in now.



The card era (early 2000s): the age of the magnetic stripe

At the start of the century, the crown jewel of consumer payments was a strip of magnetic tape on the back of a plastic card. It was a brilliant piece of engineering for its time and a gift to fraudsters, because it was static. The data on that stripe did not change. Read it once, and you could write it again onto a blank.

So that is exactly what they did. This was the golden age of the physical attack:

- **Skimming.** A small reader hidden in an ATM throat or slipped over a petrol-pump terminal, quietly copying stripe data while a pinhole camera or an overlay keypad captured the PIN.
- **Cloning and counterfeit cards.** Stripe data written onto blanks, embossed with a plausible name, and walked into a store or an ATM in another city — often another country.
- **Cheque fraud.** Still enormous in this era. Washed cheques, forged signatures, altered payees, and the classic float scam that exploited the days it took a cheque to clear.

The defining feature of the age was that value lived in data that never changed and was trivially copied. The card was a password you handed to every merchant you visited, and it never expired.

The industry's answer was **EMV — chip-and-PIN.** Instead of a static stripe, the chip generated a unique cryptogram for each transaction. Copy it and it was already worthless; the code would not validate a second time. Paired with a PIN, it broke the economics of counterfeit cards at the physical point of sale almost completely. Over roughly a decade, in every market that adopted it properly, card-present counterfeit fraud fell off a cliff.

A genuine, decisive win for the defenders. And it taught us the lesson this whole book turns on.

> **Fraud did not go away when EMV arrived. It moved. Card-present fraud fell — and card-not-present fraud rose to meet it, almost dollar for dollar in the years that followed. We didn't kill the adversary. We changed its address.**

The online shift: fraud migrates to the browser

EMV closed the door at the shop counter. But there was another door, and it had no chip reader behind it.

E-commerce was exploding at exactly the moment EMV was locking down the physical channel, and online you couldn't insert a chip. All the merchant had was the same static data EMV was supposed to make obsolete: the card number, the expiry, the three digits on the back. **Card-not-present (CNP) fraud** became the obvious next frontier, and stolen card details — worthless for making a counterfeit card — were still perfectly good for typing into a checkout page.

To feed that channel, criminals needed card numbers in volume, and two techniques matured to supply them:

- **Phishing.** The email that looks like your bank, the login page that is a pixel-perfect fake. Cheap, scalable, and aimed squarely at the weakest component in any system — the human being. Phishing has never gone away because it has never stopped working.
- **The first big data breaches.** Attackers realised they didn't need to trick a million people one at a time. They could compromise one retailer, one processor, one database, and walk away with millions of card records at once.

The strategic weakness of the whole period was **static, reusable credentials.** A card number was a secret that could be stolen once and used everywhere until someone noticed. A password was worse — chosen by a human, reused across a dozen sites, and never changed.

Defenders responded with the first generation of online controls: fraud-scoring rules on transactions, address verification, and eventually **3-D Secure** — the "verified by your bank" step that tried to put authentication back into the online purchase. It helped. It also added friction, and every point of friction is a negotiation between security and the sale. That tension — how much friction a business will tolerate to stop a loss it cannot yet see — has shaped fraud defence ever since.

The data-breach decade: your data is already out there

Somewhere in the 2010s, the breaches stopped being events and became the weather.

Not one retailer or one bank, but a relentless procession of them — hotels, health insurers, telcos, government agencies, social networks. Names, dates of birth, addresses, card numbers, and passwords by the hundreds of millions poured out of compromised systems. A mature **dark-web economy** grew up to package and sell it: card data priced by freshness and country, full identity profiles ("fullz") sold as kits, credentials traded in bulk.

This changed the game at a conceptual level, and I want to be precise about how, because most organisations still haven't fully absorbed it.

> **For any adult who has lived a normal digital life, the assumption that their personal data is secret is finished. Name, date of birth, address, past passwords, card numbers — assume it is all already in someone's database, for sale. Your defences cannot rest on knowing a secret the whole internet already knows.**

Two attack patterns industrialised on the back of this:

- **Credential stuffing.** Because people reuse passwords, a set of logins leaked from one site can be fired automatically at hundreds of others. Most fail. Enough succeed. It is cheap, automated, and endlessly patient.
- **Account takeover (ATO) at scale.** Once inside a real customer's account, the criminal inherits their trust — saved cards, established payees, transaction history that makes the fraud look normal. ATO became a major loss category and, just as damaging, a source of customer trauma that no chargeback ever fully repairs.

The defenders' answer was to stop trusting static secrets and start looking at everything around them. **Multi-factor authentication** moved from optional to essential. **Device fingerprinting, behavioural biometrics, and velocity checks** emerged — was this the usual device, the usual typing rhythm, the usual pattern, or a bot working through a list at machine speed? The industry began its slow, still-unfinished shift from *what you know* to *who you actually are and how you actually behave.*

Identity reinvented: when the person isn't real

If your data is already out there, the next logical crime is not to steal an identity — it is to build one.

Synthetic identity fraud does exactly that. Take a real but unused identifier — often one belonging to a child, or a fragment of a breach — bolt on a fabricated name and history, and patiently nurture the fiction. Open a modest account. Pay it off. Build a credit file. Let the synthetic "person" earn trust from the very institutions designed to verify them. Then, one day, borrow to the limit across every line at once and vanish. There was never a real victim to call the bank, which is precisely why it stays hidden so long. It became one of the hardest-to-detect and fastest-growing forms of fraud in the credit system, because our controls were built to check whether a person is who they say they are — not whether they exist at all.

Alongside it, document fraud evolved from the craft of the skilled forger to the output of software. Where you once needed a steady hand and a laminator, you now needed a template and a rendering engine. Fake passports, doctored bank statements, and manufactured proof-of-address documents could be generated on demand — a shift that set the stage for the deepfake documents and AI-generated identity artefacts we will come to shortly.

And a quieter category grew until it could no longer be ignored: **first-party fraud**, including so-called "friendly" fraud. This is the real customer who disputes a charge they genuinely made, claims a delivered parcel never arrived, or takes out credit they never intend to repay. There is no external attacker to catch. The account holder is the threat, which breaks the mental model most fraud systems are built on — that fraud is something done *to* the customer rather than *by* them. For many merchants, first-party losses quietly overtook the external kind.

The real-time revolution: the float disappears

For decades, defenders had a secret weapon they rarely named: **time.**

Payments were slow. Cheques cleared over days, bank transfers settled overnight in batches, and that lag — the "float" — was where fraud got caught. It gave a monitoring team the hours they needed to spot the anomaly and pull the transaction back before the money was truly gone.

Real-time payments took the float away.

Around the world, instant-payment rails went live — money moving between accounts in seconds, any hour, any day, irreversibly. In Australia the **New Payments Platform (NPP)**, with **Osko** for instant transfers and later **PayTo** for authorised debits, delivered exactly that: fast, final, always-on. It is genuinely good for the economy and for customers. It also detonated the old defensive model. When settlement is instant and irreversible, there is no window. By the time a human looks, the money is not just gone — it has already been moved through two more accounts and out.

Criminals understood the implication faster than most institutions did, and they made a strategic pivot that defines fraud today. If breaking *into* accounts is hard because of MFA and behavioural monitoring, don't break in. **Get the customer to send the money themselves.**

This is the world of **authorised push payment (APP) scams** — and it is, right now, the centre of gravity of financial crime against consumers:

- **Investment scams.** Fake trading platforms and crypto "opportunities" with dashboards that show fictional gains, engineered to trigger ever-larger deposits.
- **Romance scams.** Trust built patiently over weeks or months, then monetised through a manufactured crisis or a can't-miss investment.
- **Invoice redirection and business email compromise (BEC).** A real invoice intercepted or spoofed, the bank details swapped, and a legitimate business payment steered into the criminal's account. This one hunts businesses, and the sums are large.
- **Impersonation scams.** The "bank fraud team," the "tax office," the "police" — an urgent, frightening call convincing the victim to move their money to a "safe account" that belongs to the offender.

The cruelty of the APP scam is that every control built to verify the payer works perfectly. The customer *is* who they say they are. They *did* authorise the payment. They passed the MFA, they cleared the behavioural checks — because they were manipulated into doing so. The fraud is in the intent, not the identity, and that is a far harder thing to detect.

Behind all of it sits the cash-out layer: **money mules.** Networks of accounts — some belonging to criminals, many to recruited or coerced everyday people — through which stolen funds are layered and dispersed within minutes. The mule network is the plumbing of modern fraud, and disrupting it has become as important as stopping the scam at the source.

Defenders are adapting again: **real-time transaction monitoring** built for seconds rather than overnight batches, **confirmation-of-payee** checks that warn when a name doesn't match an account, models that score the *receiving* side of a payment, and cross-institution intelligence sharing to trace mule networks across the banks they exploit. The float is gone for good. The defence has had to learn to think as fast as the rail.

Crypto and the new rails

While instant payments transformed the movement of everyday money, a parallel financial system grew up beside it — one built on rails the old controls were never designed to touch.

Cryptocurrency introduced pseudonymous, borderless, largely irreversible value transfer. It is important to be accurate here, because the myth cuts both ways. Most crypto is not anonymous; public blockchains are, in fact, permanent and traceable ledgers. But value can cross borders in minutes with no bank in the middle, and turning it back into spendable cash is where the real vulnerability lives.

So the fraud clustered around a few pressure points:

- **Exchanges as on- and off-ramps.** The moment where crypto becomes dollars is the moment identity matters, which is why the quality of an exchange's KYC and monitoring is decisive — and why weak ones become laundries.
- **Mixers and chain-hopping.** Services designed to sever the link between source and destination, and the tactic of hopping between different coins and blockchains to shake off anyone following.
- **Ransomware monetisation.** Crypto gave ransomware its business model. Without a fast, hard-to-seize way to collect payment, the epidemic of the last decade could not have scaled the way it did.

The defensive discipline that grew in response — **blockchain analytics and on-chain tracing** — is one of the quiet success stories of modern financial crime work. Because the ledger is permanent, funds can often be followed across wallets, through mixers, and back to the exchange where a human finally tries to cash out. The chase moved on-chain, and so did the investigators. Tracing didn't die with crypto; it changed venue and, in some ways, got sharper.

The AI inflection (now): scale meets deception

Which brings us to the era we are in, and the reason this book exists now rather than five years ago.

Generative AI is not a new fraud type. It is a force multiplier applied to every fraud type that came before, and it attacks the two things that used to give the schemes away.

The first is quality. For years, the tell-tale sign of a phishing email or a scam message was that it read wrong — clumsy grammar, odd phrasing, a generic greeting. AI has erased that tell. Phishing can now be generated flawlessly, in any language, personalised at scale from breached data, and iterated instantly against whatever filter it meets.

The second, and more serious, is authenticity of the person. **Deepfake voice and video** move impersonation from the phone call to something far harder to refuse:

- A cloned voice — built from seconds of audio scraped off a webinar or a voicemail — calling finance with an urgent request in a familiar tone.
- Deepfake video convincing enough to carry a fake executive through a video call authorising a transfer that a written email never could.
- AI-generated identity documents and selfies aimed straight at the remote-onboarding checks that are supposed to prove a new customer is real.

This is the APP scam and the BEC attack given a face and a voice. Everything the last era taught fraudsters about manipulating the authorised human, AI now lets them do with terrifying conviction.

But the same technology is on our side of the table, and this is where a good defender leans in rather than despairs. AI and machine learning are how modern defence keeps pace: models that detect anomalies across billions of transactions in real time, that read the behavioural signature of a session rather than a single data point, that spot the faint pattern of a mule network forming, and that flag the synthetic identity that no rule-based check would question. The arms race has simply moved up a level — machine deception against machine detection — and the winners will be the organisations that treat AI as core defensive infrastructure, not a novelty.

The pattern

Step back from twenty-five years of detail and the same shape appears in every era.

- **Fraud migrates to the least-defended, highest-velocity channel.** EMV hardened the card counter, so fraud went online. Online authentication hardened, so fraud stopped breaking in and started persuading customers to pay. Instant payments removed the float, and APP scams filled the space the float used to protect. Each defensive win redirected the attack; it never ended it.
- **Static controls always lose eventually.** The magnetic stripe, the reusable card number, the memorised password, the overnight batch — every defence built on something fixed was, in time, copied, stolen, or outrun. Anything that doesn't change gets beaten by something that does.
- **The human is the constant target.** From the phishing email to the deepfake voice, the most reliable way past a technical control has always been to convince a real, authorised person to open the door themselves.
- **The winners build adaptive, layered defence.** No single control has ever held. What holds is depth — identity, behaviour, transaction, network, and human awareness working together, monitored in real time, and expected to evolve because the adversary certainly will.

That is the terrain. You are not defending against a list of tricks; you are up against an adaptive opponent who will always find the fastest channel you have left unwatched. The good news is that adaptive opponents follow patterns, and patterns can be mapped.

So let's map them. The next chapter lays out every major fraud type operating today — how each one actually works, and where it hits.

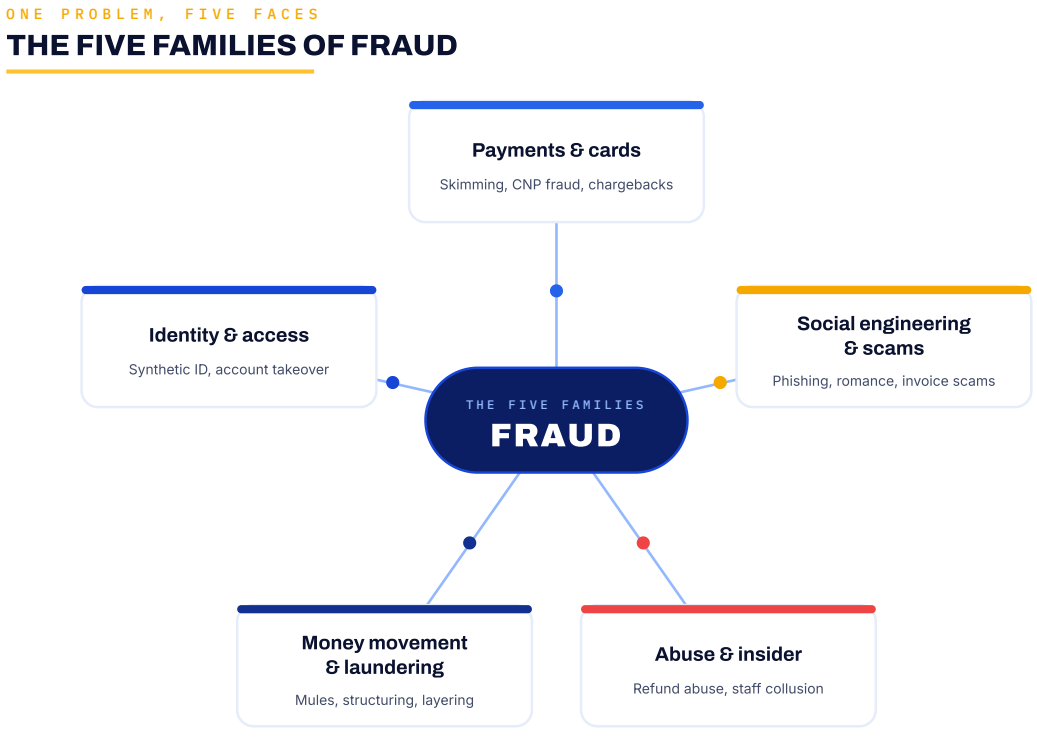
02

Part 2: The Modern Fraud Taxonomy — Every Threat Operating Today

Fraud is not one problem. It is a marketplace — with specialists, suppliers, tooling, and pricing — and the threats your business faces are the products that marketplace currently sells. To defend against them, you first have to name them accurately, because the control that stops a card-testing bot is useless against a romance scam, and the model that catches a synthetic identity will wave a business email compromise straight through.

This part is a field guide. It groups today's active threats into five families based on where they attack you:

- **Payments & cards** — abuse of the payment rail itself.
- **Identity & access** — pretending to be someone, or something, they are not.
- **Social engineering & scams** — manipulating a human into moving the money for them.
- **Money movement & laundering** — getting the stolen value out and making it clean.
- **Abuse & insider** — exploiting your own rules, incentives, and staff.



— THE FIVE FAMILIES OF FRAUD

For each type you get the same four things: how the scam works, who it targets, the tell-tale signals, and why it is hard to stop. Read it as a catalogue you can check your own exposure against — not every threat here will apply to you, but you should be able to say why for each one.

Card-not-present (CNP) fraud

How it works. A criminal uses stolen card details — number, expiry, CVV — to buy goods or services where the physical card is never presented: online, in-app, over the phone. The data comes from breaches, phishing, skimming or dark-web card shops. Because the merchant can't inspect a chip or PIN, they're relying entirely on data that has already been compromised.

Who it targets. Any merchant that accepts remote payments — e-commerce, subscriptions, travel, digital goods and ticketing are perennial favourites because the product is high-value, easily resold, or delivered instantly with no shipping delay to interrupt the fraud.

Tell-tale signals. Billing and shipping addresses that don't match; orders rushed to the fastest delivery; a single device or IP cycling through many cards; mismatch between the card's issuing country and the customer's stated location; high-value first-time orders with no account history.

Why it's hard to stop. The underlying card data is genuine — the transaction authorises perfectly at the issuer. Liability for CNP fraud typically sits with the merchant, not the bank, so you carry both the loss and the chargeback fee. Tighten checks too far and you decline good customers; loosen them and losses climb. It is a constant balancing act between fraud rate and conversion.

Card testing / BIN attacks

How it works. Before criminals sell or spend stolen cards, they need to know which ones still work. They run automated scripts that fire large volumes of tiny authorisations — often $1 or a small donation — against a merchant's checkout or payment API to see which cards approve. A BIN attack is the same idea run against a card range: taking one valid Bank Identification Number and brute-forcing the remaining digits, expiry and CVV until live cards fall out.

Who it targets. Merchants with weakly protected payment endpoints — anyone with an exposed checkout, a donation form, or an API that accepts card attempts without friction. Charities and small merchants are heavily hit because their forms are simple and unprotected.

Tell-tale signals. Sudden spikes in low-value transactions; abnormally high decline rates; sequential card numbers; a flood of attempts from a narrow set of devices, IPs or user agents; many cards sharing the same BIN in a short window.

Why it's hard to stop. It's fully automated and cheap to run, so attackers iterate faster than manual review can respond. The individual transactions are tiny, so they slip under value-based alerts. Worse, even when the testing itself costs you little, you wear the authorisation fees and the reputational hit with your acquirer — and the validated cards then come back as full-value CNP fraud elsewhere.

Chargeback fraud & first-party ("friendly") fraud

How it works. A genuine cardholder makes a genuine purchase, then disputes it with their bank to claw the money back while keeping the goods or service. Sometimes it's opportunistic ("I didn't get it"); sometimes it's deliberate and habitual. "Friendly" is a misnomer — for the merchant it is theft dressed as a legitimate dispute, and the chargeback process is weighted toward the cardholder.

Who it targets. Digital goods, gaming, streaming, gambling and travel are especially exposed because the "was it delivered?" question is murky and the customer already has what they wanted. Any merchant with weak delivery evidence is vulnerable.

Tell-tale signals. A customer with a pattern of disputes across time; claims of non-delivery on items with solid tracking; disputes filed just after a service was clearly consumed; "item not as described" on standardised digital products.

Why it's hard to stop. The transaction was legitimately authorised — your fraud models have nothing to flag at the point of sale, because there was no fraud at the point of sale. The abuse happens weeks later, inside the dispute system. Fighting chargebacks is labour-intensive, win rates are modest, and being too aggressive damages customer relationships and your standing with card schemes, which police excessive chargeback ratios.

Account takeover (ATO) & credential stuffing

How it works. Attackers gain control of a legitimate customer's account and use its standing — saved cards, stored value, trust, transaction history — to commit fraud. The most common entry route is credential stuffing: taking username-password pairs leaked from other breaches and firing them at your login at scale, betting on password reuse. Successful logins are then drained, resold, or used as a beachhead for further fraud.

Who it targets. Anyone holding accounts with value attached — banks, fintechs, exchanges, loyalty programmes, marketplaces, gaming wallets. Loyalty-point balances are a favourite because they're valuable, liquid, and customers rarely check them.

Tell-tale signals. Spikes in failed logins across many accounts; logins from new devices, impossible-travel geographies or known proxy/VPN ranges; a change of password, email or phone immediately followed by a payout or new payee; sudden draining of stored value.

Why it's hard to stop. Once inside, the attacker *is* the user — correct credentials, sometimes even the right device fingerprint if malware is involved. Blunt defences punish real customers with password resets and friction. And because breached credentials are effectively infinite and free, stuffing never really stops; you can only make your login expensive enough to attack that they move on.

Synthetic identity fraud

How it works. Rather than stealing one real person's identity, the fraudster manufactures a new one by stitching together real and fake data — often a real (frequently a child's or elderly person's) government identifier bolted onto a fabricated name, date of birth and address. The synthetic identity is nurtured over months: small credit lines, on-time repayments, building a legitimate-looking history — before it "busts out," maxing every facility at once and vanishing.

Who it targets. Lenders, card issuers, buy-now-pay-later providers and neobanks — anywhere credit or accounts are granted based on a data trail rather than a person in front of you.

Tell-tale signals. Thin or suspiciously recent credit history; an identifier with no corroborating footprint before a certain date; multiple identities sharing a phone, device, address or IP; perfectly-behaved young accounts that suddenly draw down everything.

Why it's hard to stop. There's no victim to report the fraud, because the person doesn't exist — so it often surfaces only as an unrecoverable "bad debt" rather than fraud at all. Traditional identity verification checks whether the data is internally consistent, and a well-built synthetic passes because each element is plausible. It defeats controls designed to confirm real people, because it never claimed to be one.

New-account / application fraud

How it works. The fraudster opens an account using stolen or synthetic identity data with the intent to abuse it from day one — to launder funds, receive scam proceeds, harvest a signup bonus, or serve as a disposable mule account. Unlike ATO, there's no legitimate owner; the account is fraudulent from the moment it's created.

Who it targets. Fast-onboarding fintechs, digital banks, crypto exchanges and any platform where an account can be opened in minutes and used immediately. The faster and more frictionless your signup, the more attractive you are.

Tell-tale signals. Bursts of applications sharing device, IP, address or funding source; disposable or recently created email addresses; data that verifies individually but clusters suspiciously across applications; accounts that go dormant, then activate purely to move money.

Why it's hard to stop. Onboarding speed is a competitive feature — customers and product teams both want it — and every check you add is friction that costs conversions. The identity data often verifies cleanly because it's stolen from a real person or professionally synthesised. And the harm frequently lands downstream, when the account is used as a conduit, making it easy to treat as someone else's problem.

Authorised push payment (APP) scams

How it works. The victim is manipulated into authorising a payment themselves — pushing money out of their own account to the criminal. Because the customer clicks "confirm," every technical control passes; the fraud is entirely in the deception. Common flavours:

- **Investment scams** — fake trading platforms, crypto "opportunities" and share tips showing fabricated gains until the victim tries to withdraw.
- **Romance scams** — a long-cultivated relationship that turns into requests for money for emergencies, travel or investments.
- **Task / job scams** — victims recruited into "online jobs" that require them to deposit funds to "unlock earnings."

Who it targets. Retail banking customers of every institution, and increasingly the banks and payment providers themselves, who face rising regulatory and reimbursement pressure to detect and prevent these payments.

Tell-tale signals. Payments to a brand-new payee, often followed by rapid escalation; transfers to accounts flagged elsewhere as scam-linked; a customer moving money in a hesitant, coached pattern; language suggesting investment returns or an online relationship.

Why it's hard to stop. The customer is the one authorising, so there is no compromised credential, no anomalous login, nothing technically wrong. The battleground is the customer's state of mind, which your systems can't see. Warnings are routinely overridden by a victim who has been socially engineered to distrust their own bank.

Business email compromise (BEC) & invoice/payment redirection

How it works. The criminal inserts themselves into a legitimate business payment. Either they compromise a real mailbox (via phishing or ATO) and watch for an invoice, or they impersonate an executive, supplier or lawyer using a spoofed or look-alike domain. At the critical moment they send updated "bank details," and the genuine payment lands in the fraudster's account. A common variant is the CEO-fraud "urgent, confidential" transfer request to a finance staffer.

Who it targets. Businesses of every size, their finance and accounts-payable teams, and anyone who pays invoices by trusting emailed instructions. Property settlements, large supplier payments and M&A flows are prime targets for the size of the prize.

Tell-tale signals. Last-minute changes to bank details; look-alike domains (subtle character swaps); pressure, secrecy and urgency; requests that bypass normal approval; a reply-to address that differs from the sender.

Why it's hard to stop. There's often no malware and no forced entry — just a convincing email exploiting a trusting process. It targets people, not systems, and preys on hierarchy and haste. The only reliable control is out-of-band verification of any change to payment details, and under deadline pressure that step is exactly what gets skipped.

Impersonation & deepfake-enabled fraud

How it works. The fraudster pretends to be a trusted party — your bank, a government agency, a supplier, a colleague, an executive — to extract money or credentials. The alarming evolution is synthetic media: AI-generated voice clones and video that make the impersonation far more convincing than a text email, including faked "voice confirmations" of a payment or an executive appearing live on a call to approve a transfer.

Who it targets. Consumers via impersonation of banks and government; businesses via impersonation of executives and suppliers; and increasingly, the verification controls (voice biometrics, video KYC) that were themselves meant to be the defence.

Tell-tale signals. Contact through an unexpected channel; urgency and authority pressure; requests to move money or reveal codes; audio or video with subtle artefacts — off timing, unnatural cadence, mismatched lighting; any "confirmation" that can't be independently verified.

Why it's hard to stop. The tooling has become cheap, fast and good enough to fool people, and "I heard their voice" or "I saw them on the call" is now unreliable evidence. It undermines the human-trust signals that fraud controls have historically depended on, and defences that assume a voice or face is proof of identity are being actively broken.

Money mules & mule networks

How it works. Stolen or scam money can't stay where it lands — it has to move through accounts that look legitimate. Mules are people whose accounts do that moving: some are complicit, many are recruited under the guise of a "job" or a favour, some are themselves victims. Funds are pushed through layers of mule accounts to break the trail before cash-out. Organised networks run these accounts at scale, coordinating hundreds of them.

Who it targets. Every bank and payment provider, whose accounts get co-opted as the plumbing; and vulnerable individuals — students, job-seekers, newcomers — recruited to be mules, often unaware they're committing an offence.

Tell-tale signals. Accounts that receive funds and forward them almost immediately; a mismatch between account activity and the holder's profile; many accounts sharing devices, beneficiaries or timing patterns; sudden activity in a previously dormant account; funds fanning in from many sources and out to few.

Why it's hard to stop. Mule accounts are opened with real identities — sometimes the genuine owner's — so onboarding checks pass. The behaviour looks like ordinary transfers unless you analyse the network around it, and no single account looks damning. Mules are cheap and disposable, so networks simply recruit more as fast as you close them.

Money laundering basics (placement, layering, integration)

How it works. Laundering is the process of making criminal proceeds appear legitimate, traditionally described in three stages:

- **Placement** — getting the illicit funds into the financial system (cash deposits, buying assets, loading value onto accounts).
- **Layering** — moving and splitting the money through complex transactions across accounts, businesses, jurisdictions and instruments to obscure its origin.
- **Integration** — bringing the now-clean-looking funds back to the criminal as apparently legitimate income, investment returns or business revenue.

Who it targets. Every business that moves money is a potential conduit — banks, remitters, exchanges, gaming operators, high-value dealers. You're not the intended victim; you're the machinery the launderer wants to use, and the one carrying the regulatory risk if you do.

Tell-tale signals. Transactions structured just under reporting thresholds; funds flowing through unrelated accounts or shell entities; activity inconsistent with the customer's known business; rapid movement with no economic rationale; unexplained links to high-risk jurisdictions.

Why it's hard to stop. Each individual step is designed to look mundane — the whole point of layering is that no single transaction is suspicious. Seeing it requires connecting activity across accounts, institutions and borders, which no one participant fully observes. Launderers deliberately exploit the seams between systems and jurisdictions, and they adapt faster than typologies get updated.

Crypto-specific fraud

How it works. Crypto's speed, pseudonymity and irreversibility make it fertile ground for fraud that has no clean fiat equivalent:

- **Exchange fraud** — fake or manipulated platforms that take deposits and block withdrawals.
- **Wallet drainers** — malicious contracts, phishing sites and fake token approvals that empty a victim's wallet the moment they connect or sign.
- **Mixers / tumblers** — services that pool and shuffle funds to break the on-chain trail, used to launder proceeds.
- **Pig-butchering** — a hybrid of romance and investment scam where victims are groomed over time, shown fake gains on a bogus platform, and drained when they try to withdraw.

Who it targets. Exchanges, wallets and on/off-ramps; retail crypto users; and any business bridging crypto and fiat, which inherits both worlds' risks.

Tell-tale signals. Urgency to move funds off-platform; transactions to addresses linked to known scams or mixers; token-approval requests to unfamiliar contracts; deposit-heavy accounts that never withdraw; long grooming followed by escalating "investments."

Why it's hard to stop. On-chain transactions are irreversible and settle in minutes — once the money's gone, it's gone. The ecosystem crosses borders and platforms with no central authority to freeze funds. And while the ledger is public, attribution to a real person is hard, so tracing rarely translates into recovery.

Refund, promo & loyalty abuse

How it works. Rather than breaking a rule, the fraudster exploits one. They claim refunds for items kept or never faulty, manufacture "non-delivery" claims, farm sign-up promos and discount codes across many accounts, or drain loyalty and cashback schemes beyond any legitimate use. Individually petty; at scale, and when industrialised by professional "refunding" services, materially costly.

Who it targets. E-commerce, marketplaces, subscription services, food delivery and any business running generous refund policies or acquisition incentives — the more customer-friendly your policy, the more abusable it is.

Tell-tale signals. Customers with repeated refund or "didn't arrive" claims; many accounts sharing device, address or payment method to reharvest promos; loyalty redemption inconsistent with genuine activity; referral rings crediting each other.

Why it's hard to stop. It hides in the grey zone between legitimate customer behaviour and abuse — some refund claims are genuine, and clamping down hurts real customers and conversion. The individual amounts are small enough to ignore, so it's under-prioritised until aggregate leakage becomes glaring. It exploits policies you deliberately made generous to compete.

Bonus abuse, multi-accounting & collusion (gaming/gambling)

How it works. In gaming and gambling, players exploit incentives and game mechanics. **Bonus abuse** extracts sign-up and deposit bonuses with no intention of genuine play, often across many accounts. **Multi-accounting** runs multiple identities to multiply bonuses, evade limits or gain unfair advantage. **Collusion** sees players cooperate against others or the house — soft-play in poker, chip-dumping, coordinated betting.

Who it targets. Online casinos, sportsbooks, poker rooms and gaming platforms — anywhere real money meets incentives and competitive play.

Tell-tale signals. Clusters of accounts sharing device, IP, payment method or behavioural patterns; accounts that claim a bonus and immediately cash out; playing styles that consistently favour a linked account; deposit/withdrawal patterns with no genuine gameplay in between.

Why it's hard to stop. Distinguishing a sharp-but-legitimate player from an abuser is genuinely hard, and false accusations drive away good customers. Multi-accounting hides behind shared households and devices that also have innocent explanations. Collusion requires modelling relationships between players, not just individual behaviour — and determined abusers actively disguise the links.

Insider fraud

How it works. The threat comes from inside — an employee, contractor or partner abusing legitimate access to steal funds, data or advantage. It ranges from a staff member manually processing fake refunds or approving fraudulent payments, to leaking customer data to external criminals, to colluding with fraudsters by disabling controls or waving transactions through.

Who it targets. Every organisation, but especially those where individuals hold significant access to money movement, customer data or the fraud controls themselves. Finance, operations, customer support and — dangerously — the fraud and security teams who know exactly where the gaps are.

Tell-tale signals. Access or activity outside a role's normal scope; manual overrides, exceptions and adjustments clustering around one operator; refunds or payments to linked parties; controls repeatedly disabled or bypassed by the same person; reluctance to take leave or share duties.

Why it's hard to stop. Insiders have legitimate credentials and know your controls, so their actions look authorised because they *are* authorised. Many defences point outward and assume internal actors are trustworthy. Detection depends on segregation of duties, least-privilege access and monitoring your own people — culturally and technically harder than watching outsiders.

How these connect

No serious fraud arrives as a single, tidy type. They chain. A data breach supplies the credentials for **credential stuffing**, which yields **account takeover**. The drained funds need somewhere to land, so they flow into **new-account fraud** and **money mule** networks, then through **layering** to come out clean. A **pig-butchering** scam is a **romance scam** and an **investment scam** and an **APP scam** and a **crypto** fraud, all at once. **Synthetic identities** open the mule accounts that cash out the **BEC** payment. An **insider** can quietly disable the very control that would have caught any of them.

The lesson is that treating these as isolated problems — a card team here, a scams team there, an AML function in another building — leaves the seams between them wide open, and the seams are exactly where the professionals operate. The threats are a connected system. So is the defence.

> **Naming the threat is only step one. Detection, disruption and recovery are where the real work lives — and that is the subject of the next part.**

03

Part 3: How to Stop It — A Defender's Playbook

There is no box you can buy that stops fraud. There is no policy you can write, no vendor you can sign, no certificate you can hang on the wall that makes the problem go away. Anyone who tells you otherwise is selling you the box.

Fraud is not a static threat. It is a live adversary with an economic incentive, a feedback loop, and — increasingly — automation and AI of its own. The moment you deploy a defence, the other side begins probing it. What worked in January is leaking by June. This is the single most important thing to understand as a defender: you are not building a wall, you are running a system that has to adapt as fast as the people attacking it.

That means defence is engineered, not purchased. It is layered across the entire lifecycle of a transaction — from the first time you meet a customer, through every payment they make, to the forensic reconstruction you run when something goes wrong. Each layer catches what the last one missed. No single layer is expected to be perfect, and that is the point: depth is what turns a lucky break for the attacker into a dead end.

This part is the practical core of the book. It walks through how to build that layered, adaptive defence — the model, the mechanics, the operating reality, and the ways it most commonly falls apart.

The four-stage model: Prevent → Detect → Investigate → Recover

Every effective fraud programme, whatever the industry, resolves into four stages. Treat them as a chain — because that is exactly how an attacker experiences them.

Prevent. Stop the fraud before it happens. This is your cheapest and most valuable layer: fraud that never enters the system costs nothing to investigate and nothing to recover. Prevention is identity, access, and platform hardening — making it expensive and difficult for the wrong person to get in or to act. Good prevention is invisible to legitimate customers and quietly brutal to attackers. What "good" looks like: friction is proportional to risk, not applied uniformly; controls are risk-based rather than one-size-fits-all; and you measure prevention not by how many customers you block, but by how few bad actors get through without over-penalising the good ones.

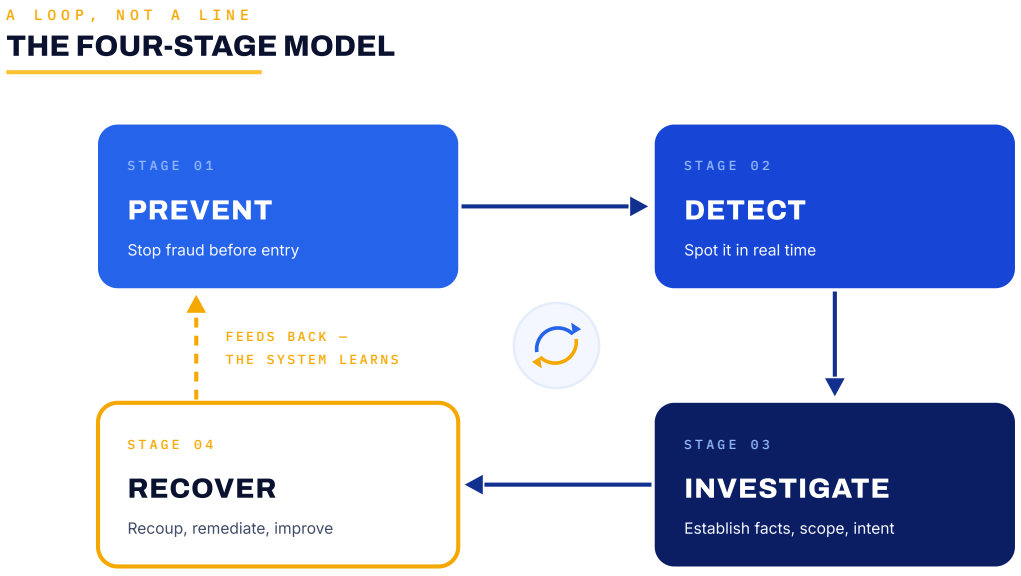
Detect. Assume prevention will fail some of the time — it always does — and catch what gets through. Detection is the engineering discipline of spotting fraud in motion: rules, models, risk scoring, behavioural and device signals. What "good" looks like: high recall on real fraud, a false-positive rate low enough that your team can actually work the alerts, and explanations attached to every decision so a human can act on it. Detection that no one can interpret is detection no one can trust.

Investigate. A detection is a hypothesis, not a verdict. Investigation is where a human — supported by good tooling — turns an alert into a decision: is this fraud, and if so, what is the full extent of it? What "good" looks like: analysts with the context and the tools to resolve a case quickly, link analysis that reveals the network behind a single event, and case management that captures a defensible record of what was decided and why.

Recover. When money has moved, the job is not over. Recovery is tracing the funds, building evidence, engaging banks and law enforcement, and clawing back what you can. What "good" looks like: the ability to reconstruct where money went across accounts and rails — including crypto — fast enough that recovery is still possible, and evidence clean enough to stand up.

> **The stages feed each other. Every investigation should teach your detection layer a new signal. Every recovery should teach your prevention layer where the hole was. A programme where these stages are run by separate teams that never talk is a programme that never learns — and an adversary that adapts faster than you do will win on that gap alone.**

The rest of this part goes deep on each stage.



— THE FOUR-STAGE DEFENCE MODEL

Prevention: identity, perimeter and platform

Prevention has three fronts: knowing who you are dealing with, controlling how they get in, and making sure the platform they get into is not itself the weak point.

Identity and onboarding

Most fraud traces back to a moment where the wrong person was let in — either a synthetic or stolen identity at onboarding, or a legitimate account later taken over. Get onboarding right and you strip out a huge share of downstream loss.

Know Your Customer and Customer Due Diligence done *well* means more than collecting a name and a document to satisfy a regulator. It means:

- **Document verification with genuine forgery detection** — checking that an ID is authentic, not just that the fields are filled in. Template matching, security-feature checks, and tamper detection, not a human glancing at a scan.
- **Liveness and biometric checks** — confirming a real, present person, not a photo, a mask, a replayed video, or a deepfake. Liveness detection is now a front line, because generative tools have made static-image spoofing trivial.
- **Device and network binding** — tying an identity to the device and network it onboarded from, so you have a baseline to compare against later. A login from a wildly different device or geography than the one that onboarded is a signal you only have if you captured it at the start.
- **Risk-based friction** — layering deeper checks onto higher-risk signups rather than punishing everyone. A low-risk customer sails through; a high-risk one gets stepped up.

The synthetic-identity problem — identities assembled from a mix of real and fabricated data — is specifically defeated at this stage or not at all, because a synthetic identity behaves perfectly normally once it is inside. Cross-referencing data points for internal consistency, and checking them against authoritative sources, is what catches an identity that has never existed as a real human.

Securing the perimeter

Even a perfectly onboarded customer can be impersonated. The perimeter is about authentication and abuse resistance.

- **Strong authentication and MFA** — but not all MFA is equal. SMS one-time codes are phishable and SIM-swappable. Push-based approvals are vulnerable to fatigue attacks. Move toward phishing-resistant factors.
- **Passkeys** — FIDO2/WebAuthn credentials bound to the device and to your domain are the strongest widely-available step forward. They cannot be phished in the traditional sense, because there is no shared secret to steal and the credential will not release for a look-alike domain. For any business moving money, a passkey roadmap should be on the table now.
- **Bot defence and credential-stuffing protection.** Attackers test stolen username/password pairs at scale against login endpoints. Without rate-limiting, device fingerprinting, and bot detection, a credential-stuffing run will quietly find the accounts where customers reused passwords. Defences include velocity controls on login attempts, challenge escalation on anomalous patterns, and detecting the automation signatures of headless browsers and scripted traffic.
- **Account-takeover monitoring** — watching for the tell-tale sequence of a takeover: a login from a new device, followed by a change of contact details, followed by a new payee and a payment. That *sequence* is far more suspicious than any single event, and catching it requires joining those events together.

Hardening the platform

This is the IT-security angle, and it is where a lot of fraud programmes have a blind spot: the application and infrastructure themselves. If your platform can be compromised, no amount of transaction monitoring will save you — the attacker is inside the system of record.

- **Secure application development** — defending against the standard classes of web and API vulnerability, because a broken access control or an injection flaw can expose account data or move money directly.
- **API security** — modern fraud increasingly targets APIs, not screens. Authentication, authorisation, rate-limiting and schema validation on every endpoint, including the ones you forgot you exposed.
- **Cloud security and secure architecture** — least-privilege access, network segmentation, secrets management, and hardened configuration. Misconfigured cloud storage and over-permissioned credentials are recurring root causes of large breaches.
- **Segregation and integrity controls** — so that even a compromised component cannot silently alter balances, payees or transaction records without leaving a trace.

Prevention across these three fronts is what determines how much load lands on your detection layer. Weak prevention floods detection with attempts it should never have had to see.

Detection engineering: the anatomy of good detection

Detection is where most of the craft lives, and where most programmes underinvest. The goal is deceptively simple — find the fraud, miss as little as possible, and don't drown legitimate customers in false positives. Achieving it is an engineering discipline.

Rules versus machine-learning models

You need both. They fail differently, and that is their strength.

- **Rules** are explicit, explainable and instant to deploy. "Block any payment over a threshold to a payee added in the last hour from a new device." Rules are excellent for known typologies, for hard policy lines, and for reacting *fast* to a fraud pattern you just discovered — you can write a rule this afternoon. Their weakness: they are brittle, they only catch what you already thought of, and they generate false positives at the edges.
- **Machine-learning models** learn patterns across hundreds of features and catch fraud that no one wrote a rule for, including novel variations. Their weakness: they need good labelled data, they drift as behaviour changes, and — if you're not careful — they become black boxes that can't explain themselves.

The mature answer is a **layered decisioning system**: fast rules for hard lines and fresh threats, models for nuanced pattern detection, and a risk-scoring layer that combines their signals into a single decision. Rules catch the known; models catch the unknown; together they cover far more ground than either alone.

The signals that matter

Good detection is built from a rich set of signals, not a single score:

- **Risk scoring** — combining many weak signals into one graded decision, so you can apply proportionate action (allow, step-up, review, block) rather than a blunt yes/no.
- **Velocity checks** — how many payments, logins, new payees, or failed attempts in a window. Fraud is frequently a *rate* anomaly before it is anything else.
- **Graph and link analysis** — connecting accounts, devices, payees, addresses and phone numbers into a network. This is how you see that forty "unrelated" accounts share a device, or that money is fanning out through a mule network. Link analysis turns isolated events into a visible structure, and it is one of the highest-leverage techniques available.
- **Behavioural signals** — how a genuine user actually behaves: their typical amounts, times, payees, navigation patterns, even typing and interaction cadence. A deviation from an established behavioural baseline is often the earliest sign of takeover.
- **Device intelligence** — fingerprinting the device, detecting emulators and remote-access tools, spotting when one device is behind many accounts or when an account suddenly appears on a new device. Remote-access-tool detection is particularly important given the rise of scams where a victim is talked through a payment on their own device.

Tuning for signal

Here is the truth about detection that vendors gloss over:

an untuned model is worse than useless, because it destroys your team's trust and buries real fraud under false positives.

Tuning is the continuous work of maximising true detections while minimising false ones. It means:

- Measuring precision and recall honestly, and choosing thresholds deliberately for the cost trade-off you actually face — a missed fraud versus a blocked good customer are not equally expensive, and the balance differs by product.
- Segmenting thresholds by risk rather than applying one global cut-off — new customers, high-value payments and unusual corridors warrant tighter settings than established, low-risk activity.
- Feeding investigation outcomes back in as labels, so the system learns from every confirmed and cleared case.
- Watching for model drift and retuning on a schedule, not waiting for losses to spike.

And detection must be **explainable**. When a model flags a transaction, an analyst needs to see *why* — which signals fired — to make a fast, defensible decision, and to explain that decision to a customer or a regulator. Explainability is not a nice-to-have; it is what makes detection operable. A score with no reasons behind it cannot be worked, cannot be appealed, and cannot be trusted.

Above all, detection is never finished. Fraud adapts; your detection must be re-tuned continuously to keep pace. A detection layer that has not changed in a year is not stable — it is decaying.

Transaction monitoring that works

Transaction monitoring is detection applied to the flow of money, and the shift to real-time payments has made it dramatically harder. When settlement is instant and irreversible, you no longer have overnight batch windows to reconsider. The decision has to be made in the moment.

Designing for real-time. Monitoring for instant payment rails has to score and decide in milliseconds, in-line with the payment, without adding friction a customer will notice. That means pre-computed features, fast lookups, and a decisioning engine that can hold and release a payment inside the payment flow — not a report that lands the next morning when the money is long gone.

Thresholds and typologies. Effective monitoring encodes the *typologies* — the recognised patterns of fraud and money laundering — as detection logic: structuring, rapid pass-through, unusual corridors, mule-account fan-out, first-party fraud patterns, scam-payment signatures. Thresholds should be dynamic and risk-based, not a single static dollar line that every fraudster quickly learns to stay just underneath.

Alerting and case management. An alert is only useful if it lands somewhere it can be worked. Good monitoring feeds a case-management system that gives the analyst the full context — the customer, the network, the history, the reasons the alert fired — and captures the decision as a defensible record. Alerts should be **prioritised by risk**, so the highest-value cases are worked first, rather than a flat undifferentiated queue.

The operating model. This is the part tooling alone never solves. Monitoring is analysts *plus* tooling: the technology surfaces and prioritises; skilled people decide. The operating model that works has:

- Clear tiers — automated decisions for the clear-cut, human review for the ambiguous, and escalation paths for the complex.
- Analysts equipped with tools that make them fast, not screens that make them slow.
- Feedback from every decision flowing back into tuning.
- Capacity planning, because alert volume is a function of your tuning — and a badly tuned system will generate more alerts than any team can ever clear, which is how real fraud slips through in the backlog.

The measure of a monitoring programme is not how many alerts it generates. It is how many *good decisions* it produces per analyst-hour, and how little real fraud slips past.

Following the money: transaction tracing and forensics

When fraud succeeds and money moves, tracing is what stands between you and a total write-off. It is a distinct discipline, and one most organisations discover they don't have exactly when they need it most.

Reconstructing the path. Fraudulent funds rarely sit still. They fan out through mule accounts, hop across banks, convert between rails, and layer through intermediaries specifically to break the trail. Tracing is the forensic reconstruction of that path — following the money across accounts and payment rails to establish where it went, how fast, and where it currently sits. Speed matters enormously: the first hours after funds move are when they are most recoverable, before they have been layered and cashed out.

On-chain tracing for crypto. When funds move into cryptocurrency, the trail does not go dark — it goes public. Public blockchains are permanent, transparent ledgers, and on-chain tracing follows funds across wallets, through mixers and bridges, and toward the exchange endpoints where they must eventually touch the regulated world to be cashed out. Clustering heuristics, known-entity attribution,

and cross-chain tracking make it possible to follow crypto in ways that are often *harder* to achieve in traditional banking. Those cash-out points — the regulated exchanges — are frequently where recovery and law-enforcement engagement become possible.

Building defensible evidence. Tracing is only worth as much as the evidence it produces. That means preserving a clean chain of custody, timestamped and reproducible analysis, and documentation that will stand up to a bank's recovery team, a regulator or a court. Sloppy evidence sinks otherwise-recoverable cases.

Supporting recovery. The output of tracing feeds directly into recovery: rapid engagement with receiving banks to freeze funds still in place, referrals to law enforcement with a package they can act on, and — where funds have reached exchanges — formal requests backed by evidence. Tracing readiness built *before* an incident is what makes recovery possible *during* one.

Responding to incidents: the first 24–48 hours

When a live fraud incident hits, the first two days decide how much you lose. A prepared team executes a plan; an unprepared one improvises while money drains. Have the plan written before you need it.

Hours 0–24: Contain.

- **Stop the bleeding.** Freeze the affected accounts, disable the compromised access, block the payee or corridor, and halt the mechanism being exploited. Containment comes before investigation — you cannot analyse your way out while money is still leaving.
- **Preserve evidence.** Capture logs, transaction records, device and session data *before* anything is reset or overwritten. Evidence destroyed in the panic of hour one is evidence you cannot recover in week three.
- **Trace immediately.** Start following the money now, while it is still in reach. Every hour of delay reduces what you can freeze.
- **Notify the right people fast.** Engage receiving banks to freeze funds still in place, alert law enforcement where warranted, and activate your internal response and communications plan. Many recoveries hinge on how fast the receiving bank is contacted.

Hours 24–48: Investigate and remediate.

- **Establish scope.** How did they get in, how far did it spread, which accounts and systems are affected, and is the attacker still active? Assume the first alert understates the true extent until you have proven otherwise.
- **Close the hole.** Remediate the root cause — the vulnerability, the control gap, the process weakness — not just the symptom. If you only reverse the transactions, the door is still open.
- **Pursue recovery.** Push the tracing and evidence into active recovery: bank freezes, exchange requests, law-enforcement referrals.
- **Capture the lessons.** Every incident is a free lesson paid for in loss. Feed the root cause back into prevention and the new pattern back into detection, so this exact incident cannot happen the same way twice.

The organisations that recover well are the ones that rehearsed. A written, tested incident playbook — with named roles, contact paths to banks and law enforcement, and pre-agreed authority to freeze and act — is worth more than any single control, because it is what turns a chaotic loss into a managed one.

A layered-defence checklist

Use this to self-assess. Honest answers only — the gaps are the point.

Identity and onboarding - ☐ Document verification includes genuine forgery/tamper detection, not just field capture. - ☐ Liveness and biometric checks defend against photos, replays and deepfakes. - ☐ Device and network are captured and bound at onboarding for later comparison. - ☐ Onboarding friction is risk-based, with step-up for higher-risk signups. - ☐ Synthetic-identity checks cross-reference data for internal consistency against authoritative sources.

Access and perimeter - ☐ MFA is in place and moving toward phishing-resistant factors and passkeys. - ☐ Login endpoints have bot defence, rate-limiting and credential-stuffing protection. - ☐ Account-takeover sequences (new device → detail change → new payee → payment) are detected as a joined-up pattern. - ☐ Remote-access-tool and emulator usage is detected.

Platform - ☐ Application and API security are actively tested against standard vulnerability classes. - ☐ Cloud configuration follows least-privilege, segmentation and secrets management. - ☐ Integrity controls prevent silent changes to balances, payees and records.

Detection - ☐ Detection combines rules (fast, explainable) and models (novel patterns) with a risk-scoring layer. - ☐ Velocity, graph/link, behavioural and device-intelligence signals are all in use. - ☐ Every detection decision is explainable — an analyst can see why it fired. - ☐ Thresholds are risk-segmented, not a single global cut-off.

Detection tuning - ☐ False-positive and detection rates are measured, and thresholds set deliberately for the real cost trade-off. - ☐ Investigation outcomes feed back as labels. - ☐ Models are monitored for drift and retuned on a schedule, not after losses spike.

Monitoring and operations - ☐ Monitoring works in real time, in-line with instant payment rails. - ☐ Known typologies are encoded as detection logic and kept current. - ☐ Alerts feed a case-management system with full context, prioritised by risk. - ☐ The operating model matches analyst capacity to alert volume.

Tracing and recovery readiness - ☐ You can reconstruct a money trail across accounts and rails, quickly. - ☐ You have on-chain tracing capability for crypto cash-out paths. - ☐ Evidence is captured to a defensible, court-ready standard. - ☐ Bank and law-enforcement engagement paths are established in advance.

Incident playbook - ☐ A written, tested incident plan exists with named roles and authority to freeze/act. - ☐ First-24-hour containment, evidence-preservation and tracing steps are defined. - ☐ Root-cause remediation, not just transaction reversal, is part of the process. - ☐ Every incident feeds lessons back into prevention and detection.

Governance - ☐ Fraud, AML and security are joined up, sharing signals and intelligence — not siloed. - ☐ Someone owns the whole lifecycle end to end. - ☐ The programme is measured on outcomes (losses prevented, recovered, decision quality), not activity.

Common failure modes

The same failures recur across organisation after organisation. See if you recognise yourself.

Static rules that never get retuned. A rule set is written, works for a while, and then is never touched. Fraud adapts around it, false positives creep up, and the system slowly decays while everyone assumes it is still protecting them. A defence that does not change is a defence that is already failing — you just haven't measured it yet.

Siloed fraud, AML and security teams. The single most damaging structural failure. The account-takeover signal lives with the security team, the payment anomaly with the fraud team, the mule-network intelligence with AML — and because they never share, the attacker who touches all three walks straight through the seams. Fraud does not respect your org chart. If your teams don't share signals, the adversary exploits the gap between them.

Buying a vendor box and never tuning it. A tool is purchased, switched on with default settings, and treated as "done." But a detection system is not a product you install — it is a capability you operate. Untuned, even excellent tooling produces noise, buries real fraud, and lulls the organisation into a false sense of coverage. The box is the beginning of the work, not the end of it.

No tracing or recovery capability. Everything points at detection, and when money finally moves, there is no one who can follow it and nothing prepared to recover it. The loss is simply written off — often a loss that fast tracing could have frozen. Recovery capability built after the incident is recovery capability built too late.

Alert fatigue. A badly tuned system generates more alerts than the team can ever clear. Analysts burn out, real alerts drown in the backlog, and eventually people start closing alerts without truly working them. High alert volume is not a sign of thorough coverage — it is usually a sign of poor tuning, and it actively *creates* the gap fraud slips through.

Treating it as a compliance box-tick. The programme exists to satisfy a regulator or pass an audit, so it is designed to *look* adequate rather than to *stop fraud*. The two are not the same. Compliance is a floor, not a defence. An organisation that optimises for the box-tick will pass its audit and still bleed money, because the fraudster does not read your policy document — they test your controls.

> **Every one of these failures has the same root: treating fraud defence as a static thing you finish, rather than a living system you run. The organisations that win are not the ones with the biggest budget or the newest vendor. They are the ones who understand that they are in an adaptive contest, and who build — and keep retuning — a layered defence that learns at least as fast as the people trying to beat it.**

That is the whole discipline in one sentence: engineer defence in depth, then never stop tuning it.

04

Part 4: Sector Playbooks — Where the Money Moves

Fraud is not one problem. The way money moves through your business shapes the way criminals attack it — a real-time payments rail, a card-not-present checkout and a crypto hot wallet each invite a different playbook. The controls that protect one can be irrelevant, or actively harmful, to another. What follows is a sector-by-sector view: the threats that dominate, and the handful of defences that earn their keep. Take what fits your model, and be honest about where you sit across more than one.

WHERE THE PRESSURE LANDS

SECTOR THREAT MATRIX

SECTOR	DOMINANT THREATS
Banks & ADIs	APP scams · Mule networks
Fintech & Payments	CNP fraud · Chargebacks · Synthetic ID
Crypto Exchanges	Account takeover · Hot-wallet theft · Illicit flows
E-commerce	Stolen cards · Account takeover · Refund abuse
Gaming & Casinos	Bonus abuse · Multi-accounting · Collusion

● = HIGHEST-LOSS THREAT FOR THE SECTOR

— SECTOR THREAT MATRIX

Banks & ADIs

Banks now fight fraud at the speed of instant payments. Once money leaves on a real-time rail, it is gone — often through a chain of mule accounts and out to crypto or offshore within minutes. The dominant threat is no longer the bank's own systems being breached; it is the customer being socially engineered into authorising the payment themselves. Authorised push payment (APP) scams — romance, investment, invoice redirection, impersonation of the bank or a government agency — sidestep every authentication control because the genuine customer is doing the pushing.

The defences that matter most:

- **Real-time payment interdiction.** Score payments before they settle, not after. Hold, delay or step up on high-risk signals — new payee, unusual amount, out-of-pattern device or session behaviour.
- **Mule detection on the receiving side.** The industry over-invests in the sender and under-invests in the beneficiary. Watch for rapid in-and-out flows, sudden dormant-account reactivation, and fan-in from many unrelated senders.
- **Dynamic, contextual scam warnings.** Generic "are you sure?" prompts are noise. Tailor the intervention to the scam pattern the payment resembles.
- **Insider risk controls.** Privileged access to accounts and customer data is a standing exposure; monitor staff activity, enforce least privilege, and alert on unusual lookups.
- **Cross-institution intelligence.** Mules and scam proceeds move between banks; shared signals close the gaps a single view cannot.

Fintech & Payments

Fintechs live and die on a tension that older institutions can defer: the trade-off between blocking fraud and approving good customers. Every control you tighten costs conversions and, at scale, revenue. The threats cluster at two points — the front door and the transaction. Card-not-present (CNP) fraud and the chargebacks that follow it hit the transaction; synthetic identities and mule onboarding hit the door, where fabricated or stitched-together identities pass KYC and seed later abuse.

The defences that matter most:

- **Risk-based onboarding.** Layer device intelligence, email and phone age, behavioural signals and document checks. Synthetic identities look clean on paper and fail on correlation.
- **Manage the false-decline problem deliberately.** Track approval rate and false-decline rate as first-class metrics alongside fraud loss. A control that stops fraud but strangles growth has failed.
- **Chargeback and dispute analytics.** Feed dispute outcomes back into your scoring. Chargebacks are labelled fraud data you have already paid for — use them.
- **Controls that scale with volume.** Build for automated, real-time decisioning with human review reserved for genuine edge cases. Manual review does not survive growth.
- **Step-up, don't block.** Reserve hard declines for the clearest cases; use friction (3DS, verification) as a graduated middle path.

Crypto Exchanges & Digital Assets

Crypto platforms carry the operational risk of a bank and the finality of cash. Transactions are irreversible and pseudonymous, so a successful fraud or theft is rarely recoverable — which makes prevention and speed of response everything. The headline threats are account takeover (ATO) leading to instant withdrawal, and platform-side compromise of hot wallets and signing infrastructure. Layered over both is the compliance exposure: illicit flows and interaction with sanctioned or high-risk addresses.

The defences that matter most:

- **Hot-wallet and key security.** Minimise hot-wallet balances, enforce multi-signature or MPC signing, and separate the systems that can move funds from everything else.
- **Withdrawal-time controls.** ATO shows itself at withdrawal. Enforce hold periods on new withdrawal addresses, step up on behavioural anomalies, and alert on drain patterns.
- **On-chain analytics and tracing.** Screen deposit and withdrawal addresses against known illicit clusters, mixers and sanctioned entities in real time; retain the ability to trace flows after the fact.
- **Sanctioned-address and illicit-flow screening.** Treat AML screening as a live control on every transaction, not a periodic report — exposure here is both a loss and a regulatory event.
- **Hardened account security.** Phishing-resistant MFA, withdrawal allowlists, and anomaly detection on login and API-key activity.

E-commerce & Marketplaces

E-commerce absorbs fraud from every direction at once, and the checkout is the pressure point. Stolen-card CNP fraud drives chargebacks; account takeover turns loyal customers into attack surface; and a large share of loss is not "criminal" at all but abuse — friendly fraud (disputing legitimate purchases), and refund, return and promo-code exploitation. Marketplaces add the complication of policing both buyers and sellers, including collusion between them.

The defences that matter most:

- **Bot defence at checkout and login.** Automated card-testing, credential-stuffing and inventory-hoarding bots are the first wave. Rate-limit, fingerprint and challenge before they reach payment.
- **Risk scoring at the transaction.** Combine device, behavioural, shipping-versus-billing and velocity signals to score orders; route the risky ones to review or step-up, not a blanket block.
- **Account-takeover protection.** Monitor for credential stuffing, sudden shipping-address changes and unusual order patterns on established accounts.
- **Abuse and policy analytics.** Track refund, return and promo-code behaviour at the customer level. Serial abusers show clear patterns; friendly-fraud repeat offenders do too.
- **Clean dispute evidence.** Capture device, delivery and interaction data to win chargeback representments and deter opportunistic disputes.

Gaming, Gambling & Online Casinos

Gambling platforms combine fast, high-volume money movement with strong incentives to game the system — a natural target for both fraudsters and money launderers. Deposits, wagers and withdrawals move quickly, and the product itself can be abused to move value between colluding accounts. The dominant threats are bonus abuse and multi-accounting (one person behind many identities to farm promotions), collusion and chip-dumping (deliberately losing to shift funds to an accomplice), and the use of the platform as a laundering layer — deposit, minimal play, withdraw as "winnings".

The defences that matter most:

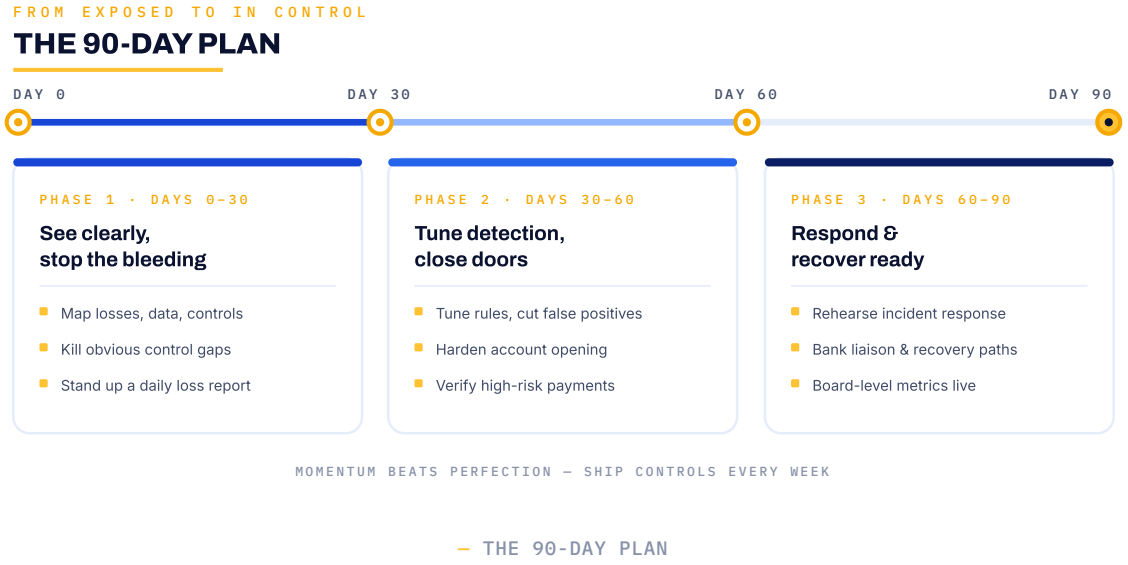
- **Multi-accounting and linkage detection.** Correlate device, payment instrument, behavioural and network signals to unmask one actor behind many accounts.

- **Collusion and chip-dumping analytics.** Analyse play patterns for improbable loss transfers, coordinated table presence and unnatural betting behaviour.
- **Bonus and promotion abuse controls.** Model expected versus actual promotion economics; flag accounts whose only activity is extracting bonus value.
- **AML-grade money-movement monitoring.** Watch for deposit-minimal-play-withdraw patterns, mismatched deposit and withdrawal methods, and velocity that signals layering.
- **Responsible-gaming and KYC integration.** Robust identity and source-of-funds checks close the door multi-accounting and laundering both rely on.

05

What to Do Next — A 90-Day Action Plan

You cannot fix everything at once, and you should not try. The plan below sequences the work so that every 30 days produces something real: first clarity, then tuned detection, then the ability to respond and recover. Adapt the specifics to your sector using the playbooks above.



— THE 90-DAY PLAN

Days 0–30 — See clearly, then stop the bleeding

Map how money actually moves. Diagram every inbound and outbound flow — rails, payment methods, third parties, settlement timing. You cannot defend a path you have not drawn.

Inventory your controls against those flows. Mark where you score, where you step up, where you block, and — critically — where you do nothing.

Rank exposure by irreversibility and speed. Instant, irreversible outbound paths are your highest priority. Money you can claw back is a lower-order problem.

Pull your loss and dispute data. Chargebacks, confirmed fraud, scam reports, write-offs. Find the two or three patterns driving most of the loss.

Ship quick wins. Velocity limits on new payees, holds on first withdrawals to new destinations, MFA on high-risk actions, basic bot defence at login and checkout. These are cheap and immediate.

Days 30–60 — Tune detection and close the doors

Tune your rules and models against real outcomes. Measure false positives honestly. A control drowning your team in noise is a control that will be switched off.

- **Uplift monitoring toward real time.** Move the decisions that matter from after-the-fact reporting to at-the-moment scoring and interdiction.
- **Close identity and access gaps.** Strengthen onboarding against synthetic and stolen identities; enforce least privilege and monitor privileged/insider access to funds and customer data.
- **Instrument the growth trade-off.** Stand up approval rate, false-decline rate and fraud loss on one dashboard so you can see the whole balance, not one side of it.
- **Add feedback loops.** Route confirmed fraud and dispute outcomes back into your scoring so the system learns.

Days 60–90 — Get ready to respond and recover

- **Build tracing and recovery readiness.** Know, in advance, how you freeze, recall, trace and escalate — internally, to receiving institutions, to law enforcement, and (for digital assets) on-chain. Speed is everything once funds move.
- **Write and rehearse an incident playbook.** Define who decides, who acts and who communicates when a fraud event or breach hits. Run a tabletop exercise against a realistic scenario.
- **Establish your metrics baseline and review cadence.** Fix the numbers you will manage to, set a monthly review, and hold it.
- **Iterate deliberately.** Retire controls that only generate noise, double down on what catches real loss, and feed the next quarter's priorities from what you have learnt.

> **The goal of ninety days is not a finished defence — there is no such thing. It is a living system: instrumented, tuned to your actual losses, and able to respond when something gets through.**

06

A Note on the Future

The fundamentals of fraud do not change — deception, misdirection, the exploitation of trust and speed. What changes is the tooling on both sides, and it is changing quickly.

AI is now in the attacker's hands. Convincing phishing at scale, synthetic identities that survive scrutiny, deepfaked voices and faces for impersonation and verification bypass, and the automation of what used to be labour-intensive social engineering. The same technology strengthens the defence — better anomaly detection, faster pattern recognition across noisy data, adaptive scoring that learns as fast as the threat. This becomes an arms race of models, and the side with better data and faster iteration wins.

At the same time, money keeps getting faster and more embedded. Instant payments, finance stitched invisibly into non-financial products, and the continued rise of tokenisation and digital assets all compress the window between fraud and irreversible loss. Controls designed for a world of overnight settlement and clawbacks do not survive contact with rails that settle in seconds and cannot be reversed.

This is why the era of the static control is ending. A rule set written last year, a threshold fixed at go-live, a policy reviewed annually — these decay the moment the environment moves, and it is always moving. Defence has to be engineered, monitored and adapted like any other live system, because that is exactly what it is up against.

The organisations that come through this well will not be the ones with the thickest compliance folder. They will be the ones treating fraud defence as an operational capability — instrumented, staffed, and improving every month.

07

About Financial Crime Advisory

Financial Crime Advisory is an Australian financial-security firm. We engineer and run the defences that protect any business that touches money — fraud prevention, transaction monitoring and tracing, and IT and cyber security — across banking, fintech, crypto, e-commerce, gaming and beyond.

The difference is in that word "run". We do not hand you a report and walk away. We build the controls, wire them into how your money actually moves, and stay to operate and tune them. We find the holes the Big Four leave behind — the gaps between the diagram and the reality — because we work at the level of systems and money flows, not slideware.

You work with senior specialists who have spent careers on this, not a rotating bench of juniors. No lock-in, no theatre — just defences that hold.

If anything in this book landed close to home, let's have a conversation. You can reach us at **financialcrimeadvisory.com.au**.