The Cat and Mouse Game: Why card issuing risk management must evolve

sardine

Executive Summary

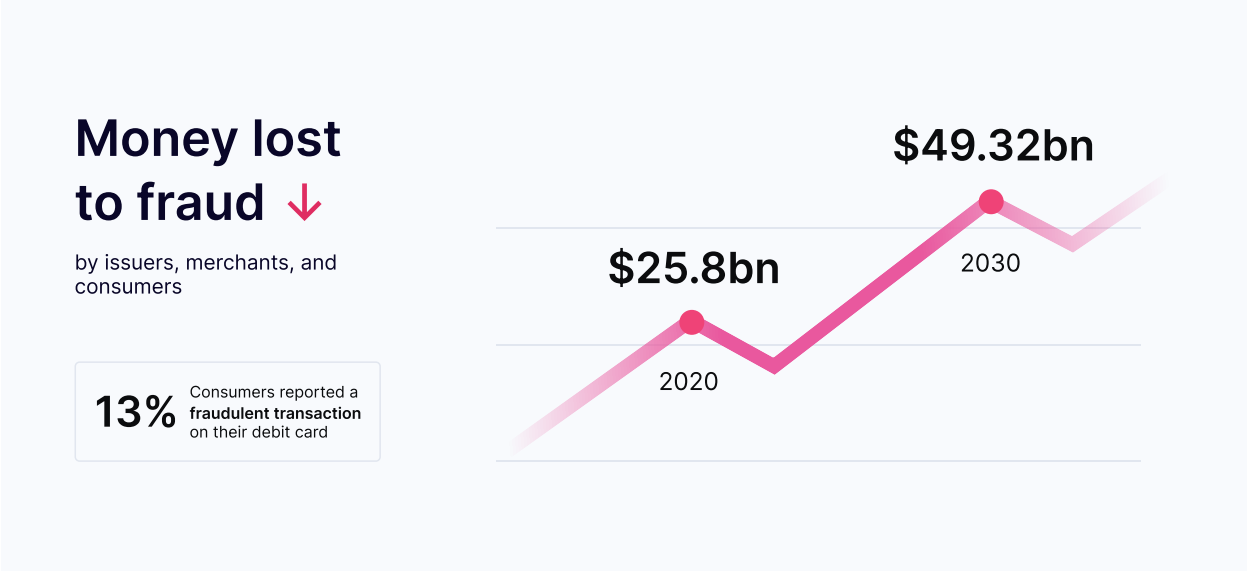
As every company becomes a Fintech company, card issuing has become a crucial brand revenue driver. Revenues for non-bank card issuers topped $22bn in 2021 and are expected to 3x by the end of 2024. Card issuers know that the faster they can onboard a user and have them make the first transaction, the more likely they are to see that customer become active. This has created an industry drive to remove friction driven by digital e-KYC.

Sponsor banks have enabled this revolution but face increasing scrutiny from state and federal regulators. The new business model has also led to a dramatic increase in fraud and economic crime which has become the single largest challenge for card issuers. Card issuers face a choice of adding friction which reduces fraud but could reduce revenue, or facing the user churn and loss of trust that comes with fraud.

Or do they?

The rise of digital account opening, accelerated by the pandemic, made fraud easier, global, and harder to detect. Every card issuer faces identity theft, scams, and account takeover risk levels. The issue is compounded by fraud tools and models built before the digital era struggling to keep pace with the emerging threat vectors.

Card fraud has become an exponentially growing and the most significant challenge facing card issuers since:



Reference: MoneyTransfers

A little bit of friction can be a good thing.

The best drivers win the race by slowing down at the right moment. The right amount of braking for the corner, weather, and situation all optimize their overall speed. The best card issuers convert users by obsessing over when to add and remove friction depending on the user, data, and context.

There is no one size fits all solution for friction or fraud.

Card issuers are challenged to build sophisticated rules, machine learning, and fraud operations around a patchwork of tools and data providers. But the issue many issuers face as they are still flying blind, dealing with black box risk models that worked in silos.

Issuers need a digital-first solution that is more comprehensive, considering fraud and AML together (FRAML) and bringing all data sources together into a single rules engine, dashboard, and API with no more black boxes.

Card issuers can increase conversion, increase share of wallet and substantially reduce the manual cost and complexity of wrestling with fraud and economic crime by partnering with Sardine.

In this report

1. The card issuing opportunity and fraud risks
2. How digital shifted the economics of card issuing and card fraud
3. The challenges card issuers face
4. The most common card issuing fraud typologies and their evolution
5. How detecting more fraud creates less friction and more revenue
6. The requirements card issuers have to balance friction and fraud
7. Sardine moving faster; together for card issuers

1. Card issuing is a critical revenue and growth opportunity for any brand but creates hidden risks

Every company will be a Fintech company. But not every company has a “PhD in financial crime detection.”

Cards are no longer the exclusive property of banks or large companies like airlines and have become more ubiquitous in the last decade. Fintech wallets, marketplaces, and e-commerce platforms are launching debit and credit cards to solve new consumer and business problems. The Fintech boom created new infrastructure and providers that reduced the cost, time, and complexity of getting products into the market.

The card is the natural starting point because they are widely accepted and come with an inbuilt business model; interchange. Interchange, also known as swipe fees, are paid by merchants to accept card payments (typically between 0.3 and 3% of a transaction, depending on the type and geography).

The key metric many card issuers live by is conversion. Any company issuing a card must open an account for their user and ensure they can successfully pay. They will generate more revenue if they can successfully open accounts and ensure the user chooses their card to transact over the competition.

Financial crime creates two primary issues for card issuers.

1. Direct losses. Card issuers are liable for refunding the cardholder in most instances. If fraud has occurred, the issuer is out of pocket.
2. Indirect costs. Like hiring more staff for investigations, finding chargeback evidence spending more on technology, and increasingly facing pushback from payment providers, banks, and 3rd parties.

The pushback from other card providers and 3rd parties can be especially damaging to card issuers because it reduces conversion over time. Merchants will begin to block transactions from card issuers if they see high rates of fraud coming from that type of card. In the first instance, card issuers are tempted to add friction to the process to reduce fraud, but in doing so damage their conversion and revenue far more than fraud.

This is because often, the historic way to catch fraud meant stopping lots of good transactions to catch the bad ones (false positives). If you have to stop 10 good transactions for 1 fraudulent transaction, you'd have a false positive ratio of 10:1. Reducing this number is critical. But the catch-22 is simply removing all friction and control will spike the fraud rate resulting in other merchants and 3rd parties blocking transactions.

The counterintuitive insight is that fraud and conversion are the same thing. All fraud problems are data problems aimed at getting more fine-grained, more accurate data about what is a risk and what is not.

2. Mobile and Digital made card-issuing much more economic for businesses and criminals

2.1. The rise of digital reduced the financial services cost structures

The impact of digital channels, such as mobile and online, on financial services cannot be understated. Financial services became much more accessible, inclusive, and real-time. Digital also substantially reduced the cost of distributing financial services, especially via credit and debit cards.

Before 2010 getting new financial products to market would take, on average, 12 months and start at $500k to $1m for launch. Innovation meant having a mobile app that distributed the same old financial products from the same old brands.

The first wave of the internet saw internet-only banks like ING emerge or companies like Capital One, who are good at the traditional product set. But the products were loans, credit cards, debit cards, checkings, and savings.

However, new issuer processors (providers who supply technology and access to card-issuing) and new program managers (Banking as a Service or BaaS providers) changed the business model by:

1. Reducing the time to market
2. Reducing the CapEx (upfront cost)
3. Reducing the Opex (maintenance cost)
4. Enabling card issuers to become more financially inclusive

The issuer processors and new BaaS providers built API-first, developer-friendly tools. They brought together a network of 3rd parties. The rest was that a new card issuing program could sometimes have a live working card within ~8 weeks and for a flat monthly SaaS fee.

By reducing the cost and time it took to market, entrepreneurs and brands could serve traditionally “high-risk” and less profitable migrant populations, low-income segments or growing businesses. Digital reduced the cost of acquisition (CAC) and cost to serve (CTS) in issuing cards.

2.2. Digital KYC and e-KYC reduced the cost and time it takes to onboard new users

Card issuers, and brands must “Know Your Customer” (KYC) both to comply with national laws and as a control to prevent known fraudsters, criminals, and bad actors from gaining accounts and using the financial system for crime.

A potential customer is asked to give evidence of their legal identity and proof of address at account opening. Legal identity documents include photo IDs like passports, driver's licenses, and national ID cards and are documents issued by a government. The definition of "identity" in this sense is the one the government you're a citizen of recognizes you by.

The bank or Fintech company will then examine these documents and any proof of address for their authenticity before opening an account. Historically this happened at a branch, but today this is most often in the mobile app and powered by Fintech infrastructure companies like Alloy, Onfido, Socure, and Sardine*.

Once these documents are collected and reviewed for authenticity, the Fintech company or bank performs checks for economic crimes.

There are three main types of economic crime.

1. Money laundering (Criminals moving money through the system)
2. Sanctions evasion and corruption (Individuals or corporations moving money that should not be allowed to or taking bribes)
3. Fraud (Attempting to steal or scam money from someone else)

Historically, to get a debit or credit card, a customer must prove their identity and address through physical documents, either by mailing copies or attending a physical retail location to present them. This was not only time-consuming, but it was also high friction. Many customers don't have paper documents lying around.

Instead of requiring customers to enter a branch, they could apply via their mobile phone in real time.

This

1. Reduced the cost of opening an account
2. Increased the conversion of customers
3. Helped a generation of companies quickly gain adoption

The pandemic became a massive accelerating force in this overall trend as consumers and businesses who relied on branches now had to open an account digitally. Issuers faced unprecedented growth levels for eKYC and digital customer onboarding.

2.3. Criminals exploited these cost reductions to scale their attacks

The same convenience that benefited consumers benefited criminals who could leverage:

- Remote onboarding: Before digital onboarding and eKYC, a fraudster or criminal had to either visit a branch or successfully take over an account opened at a branch. eKYC allowed a fraudster or criminal to use stolen credentials to apply remotely from anywhere in the world.
- Dark web stolen identities: Large-scale database hacks like Sony, Target, and LinkedIn leaked user identities online that can be bought cheaply.
- Low-cost labor: By operating remotely, fraudsters can exploit low-cost labor anywhere in the world. Additionally, criminal networks advertise "working from home" opportunities to recruit unwitting but well-intentioned individuals to perform a small part of a wider task.

Modern technology enables mass automation: Modern technology enabled large-scale spam and phishing attacks where a low success rate doesn't matter. If a fraud ring can send 100m emails, only a handful need to be exploited for that to be worthwhile.

3. Financial Crime has now become the most significant challenge for card issuers

The statistics are staggering

- In 2020 $25.8bn was lost to fraud by issuers, merchants, and consumers
- This is expected to rise to $49.32bn by 2030
- SAR fillings have increased by 15.1% YoY for the past 5 years according to the FBI
- 13% of consumers reported a fraudulent transaction on their debit card

There are a series of challenges that issuers face.

3.1. Conversion is mission critical and creates a friction vs fraud tradeoff

Every user onboarded creates cost, but issuers only receive revenue when a user begins a transaction. Issuers know that if the sooner they get a customer into the service and spending, the more likely they are to have an active user.

The most important metric to grow and drive revenue from a card-issuing product is conversion at account onboarding. Card issuers can see 60% or higher drop-off averages during the process and fight to remove friction.

3.2. Fraudsters attack new programs first

Fraudsters target small and non-bank programs because they have a higher success rate. Younger programs may not yet have a fully operational fraud and compliance function or be able to spot the signs of fraud in their service.

3.3. Financial crime prevention providers create an integration problem

Fraud prevention providers often specialize in a subsection of the value chain. For example:

- Documentary and eKYC providers capture documents and guide users through onboarding

- Data enrichment providers help verify real entities, email addresses, and mobile numbers
- Transaction monitoring providers help see a transaction, manage a case and raise a SAR but data is often siloed from fraud
- Consortia of financial institutions help card issuers identify and screen known bad actors
- Open Banking solutions help provide accurate account data about user behavior or history
- Device intelligence companies identify devices that displace patterns consistent with fraud in e-commerce
- Behavior Biometrics providers help identify user behavior that is suspicious or high-risk

Providers aren't designed to work together: A sophisticated fraud and compliance stack can require 10 to 15 providers. These solutions are typically not designed to work together and create duplication. Multiple providers also create problems for operational teams who have to create rules or apply custom machine-learning models in multiple places.

If the providers don't share data, models are impossible to optimize, and operational teams lack a single dashboard and data set. This degrades performance and creates visibility gaps that fraudsters can exploit. It also creates costly manual work for operations teams. Time spent using spreadsheets to paper over cracks in integration is time not spent investigating fraud.

3.4. Traditional controls are insufficient

Traditional controls are often not comprehensive and fail to manage the evolving digital nature of fraud.

Card programs often use onboarding as their key control: Onboarding is a critical moment to capture user data and history, but it may only be relevant at that point in time. User identities can be stolen, accounts can be taken over, and fraudsters know this is where most of the controls are placed. This leads to applying too much friction at onboarding or accounts that suddenly "go bad" after long dormant periods.

Card issuers lack the right friction and the right time and controls that are applied throughout the customer lifecycle.

Fraud systems often rely on transaction data as a key control: When a card issuer suspects fraud, they may block a transaction. This can create significant friction for good users and a high rate of false positives, creating lost revenue. Card issuers often lack the ability to build user scores and profiles over multiple transactions and interactions.

Fraud systems don't talk early or often to AML systems: Money laundering, sanctions, and terrorist financing (TF) activity often first appear as a simple fraud hit. Traditionally these are separate, siloed parts of the organization with different processes and communication priorities. Suppose fraud systems do not escalate an alert to the AML systems in time. In that case, it leads to a considerable backlog of AML alerts to be reviewed by compliance teams and potentially significant issues for card issuers and their sponsor banks.

Additionally, compliance is dictated by the rule of 30/30/30.

SAR rules require a SAR to be filed no later than 30 calendar days from the date of the "initial detection of facts that may constitute a basis for filing a SAR." Anyone with SAR requirements may file SARs for continuing activity after a 90-day review, with the filing deadline being 120 days after the previously related SAR filing date.

3.5. Financial crime evolves, requiring constant R&D; self-build creates a cost problem

No solution is ever as good (or expensive) as a bespoke build: Card issuers may prefer to self-build to solve the challenge presented by a patchwork of providers. Like a custom-tailored suit, it will fit their use case perfectly initially, but because fraud evolves, the software and build degrades over time. Fraud prevention and detection requires consistent R&D effort and is a specialism.

This leads to card issuers investing in up-front build but often being unable to maintain consistent R&D; this, too, is exploited by fraudsters.

3.6. Many providers create data lock-in and black boxes

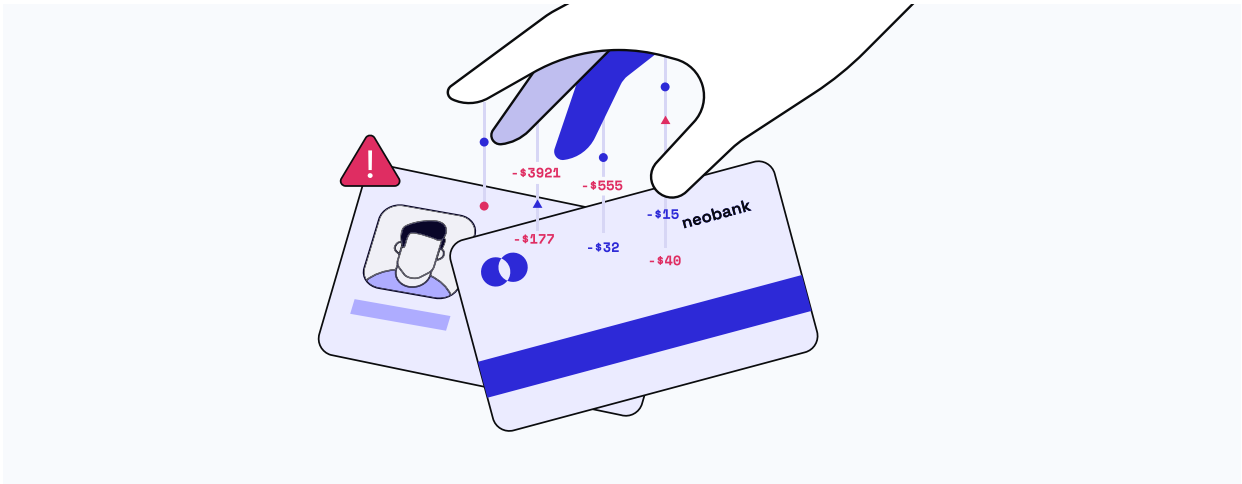
Many card issuers have a unique understanding of their fraud risk and can often create better rules and machine learning if they can pull all of their data together to identify patterns better. However, many providers don't provide easy access to this data. Additionally, some providers simply return scores or metrics without a clear chain of evidence about how they got to that result.

3.7. Losses are trending to sit with issuers instead of merchants; liability increasingly shifts

As fraud in e-commerce and digital continues to rise, merchants in physical and e-commerce are implementing services like 3D secure. 3D secure is a form of step-up verification that requires the cardholder to provide additional authentication at checkout for a payment to be complete. This is a one-time password (OTP) sent to the user or biometric authentication (e.g., thumbprint or Face ID).

When completed, the liability to cover fraud losses shifts from the merchant to the card issuer.

4. The 10 Common Card Issuing Typologies



As long as companies have sent plastic cards to consumers to make payments, fraudsters have tried to take advantage of payment methods for their benefit.

Understanding the evolution of these attacks is helpful since many are still prevalent, and these types of financial crime (typologies) still impact issuers, merchants, and consumers today.

We can better understand the most effective countermeasures by understanding the attack.

4.1 Card Present Fraud

Card Present Fraud is when a stolen or counterfeit card is used for a transaction where the card is physically present. This type of fraud peaked in the early 2000s as more businesses started to accept card payments, making it easier for fraudsters to exploit vulnerabilities in the system.

One of the key milestones in the fight against Card Present Fraud was the introduction of the EMV (Europay, MasterCard, and Visa) chip technology. This innovative solution replaced the traditional magnetic stripe, prone to skimming and cloning, with a more secure, encrypted chip. As a result, counterfeit card usage drastically decreased, and fraudsters were forced to look for new ways to deceive the system.

As technology continued to advance, so did the tactics employed by criminals. They focused on

- **Compromising point-of-sale (POS) systems** and using stolen card data for card-not-present transactions, like online shopping.
- **Shoulder surfing** to steal cardholder's PINs during transactions, enabling them to commit Card Present Fraud.
- **High-risk merchants remain an issue.** Gas stations and ATMs remain popular targets for Card Present Fraud, as criminals can install skimming devices relatively easily.

4.2 Card not present fraud

Card Not Present (CNP) Fraud is a type of financial crime that occurs when stolen or unauthorized card information is used to conduct transactions without the physical card being present. This fraud is most commonly associated with online shopping, phone orders, and mail orders, where the merchant cannot verify the card or the cardholder's identity in person.

4.2 Card not present fraud

As physical card security improved, fraudsters shifted their focus to online transactions where cards aren't physically present. Card Not Present (CNP) Fraud skyrocketed, becoming the new battleground in the war against financial crime.

As the world has become increasingly digital, CNP Fraud has grown exponentially, partly due to the enhanced security measures implemented for card-present transactions, such as the adoption of EMV chip technology. To combat CNP Fraud, card issuers, and merchants are adopting various security measures like two-factor authentication, CVV verification, and advanced fraud detection algorithms that monitor transaction patterns and flag anomalies in real-time.

Noteworthy emerging challenges:

- **Small businesses** that often lack sophisticated fraud controls
- **E-commerce**, where conversion and experience are often preferred over high decline rates at checkout
- **Cross-border transactions** lack consistent security measures and create delays in the currency conversion process that are exploited by fraudsters

4.3 Identity theft

As credit and debit cards gained popularity in the late 1980s, fraudsters quickly realized the potential for exploiting stolen personal information. This led to a surge in identity theft, with criminals using pilfered data to apply for new cards or hijack existing accounts.

This growing threat forced card issuers to take action, investing in security measures and authentication processes to protect customers and their businesses. The industry has evolved its approach from basic security features like signature panels to more advanced technologies, such as EMV chip cards and biometric authentication.

However, with the rise of digital transactions and card-not-present fraud, identity theft poses a significant challenge to card issuers. Today's fraudsters leverage sophisticated techniques like phishing and social engineering to compromise sensitive data, making it essential for card issuers to stay vigilant and adaptive.

Noteworthy emerging challenges:

- **Data breaches made 100s of millions of records available for purchase.** Breaches and hacks involving financial institutions and retailers can expose cardholders' information
- **The dark web simplifies buying stolen identities.** Fraudsters now had a single, global marketplace, could operate anonymously, and buy any other tools they needed for hacking or scams in the same place.
- **Synthetic identity theft,** where fraudsters create fake identities using a mix of real and fabricated information, had started to rise, exploiting the data gaps

4.4 Account Takeover

Account Takeover (ATO) traces back to the early days of online banking and e-commerce when cybercriminals began exploiting vulnerabilities in the system to gain unauthorized access to users' accounts. As digital transactions surged, so too did the prevalence of account takeovers.

Nearly 1 in 4 adults in the US have had their account taken over by a fraudster; since 2019, attacks are up 3x, and in 2021, losses increased by 90%.

422,143,312

Total ATO Victims in 2022

Compounding this issue is that account takeovers (ATOs) are notoriously hard to detect effectively.

Fraudsters take a stolen password (from scams like Phishing or buying online from the dark web after a data breach) and may even log in to customer emails to verify with secure one-time passwords (OTPs). This threat continues to evolve as fraudsters use more sophisticated tools to take over accounts, and the traditional ones, like simple scams, remain effective.

Noteworthy emerging challenges:

- **Remote access attacks:** Malicious software is used to remotely access and control victims' devices, allowing criminals to access sensitive information and take over accounts without the user's knowledge
- **SIM swapping:** This technique involves hijacking a victim's phone number to intercept SMS-based two-factor authentication codes, rendering this security measures less effective.

- **AI-powered attacks:** Artificial intelligence is leveraged to automate and scale account takeover attempts, enabling criminals to target a larger number of victims simultaneously.

4.5 Application Fraud

Application fraud refers to applying for a credit or debit card. In the past, criminals would submit fraudulent applications using false or stolen identities to obtain credit cards, taking advantage of paper-based systems and manual identity checks that left room for human error.

With the advent of the digital era, the landscape has shifted significantly. The speed and ease of online applications have attracted a larger audience and made them more susceptible to fraud. Cybercriminals now exploit the digital space to submit multiple applications using sophisticated techniques such as identity theft, synthetic identities, and falsified information.

Noteworthy emerging challenges:

- **Targeting non-banks:** The increasing use of Fintech companies for debit and credit cards has led fraudsters to target these issuers, where cybercriminals exploit a lack of sophistication in some early-stage companies to commit application fraud.
- **Social engineering:** Criminals exploit social media platforms to gather personal information about their targets, using it to create convincing applications and defeat identity checks.
- **AI-generated profiles:** Artificial intelligence creates realistic, yet fake, online personas that give legitimacy to fraudulent applications and can evade detection systems.

4.6 Card Skimming / Shimming

Card skimming has been a persistent challenge for the card-issuing industry since the 1990s. This fraud involves capturing cardholder data from a card's magnetic stripe using a skimmer, often installed on ATMs, gas pumps, or point-of-sale terminals.

In the early days, skimming devices were relatively large and conspicuous. However, as technology advanced, skimmers became smaller and more

sophisticated, making detection increasingly difficult. Today, criminals utilize advanced skimming techniques, such as shimming, which targets chip-enabled cards by intercepting data during transactions.

To combat this threat, card issuers have introduced security enhancements, such as EMV chip technology, which provides an additional layer of protection against skimming. However, with the rise of online transactions and digital wallets, the focus has shifted toward combating other types of fraud, such as account takeover and application fraud.

Noteworthy emerging challenges:

- **Shimming:** EMV chip technology has given rise to shimming, where criminals use ultra-thin devices to intercept chip-enabled card data during transactions, bypassing the added security.
- **E-skimming:** This involves compromising e-commerce websites to capture cardholder data during online transactions, extending the reach of skimming to the digital realm.
- **Miniaturization:** Skimming devices have become increasingly smaller and discreet, making them more challenging to detect when installed on ATMs, gas pumps, or point-of-sale terminals.

4.7 Synthetic identity fraud

Synthetic identity fraud first appeared in the early 2000s as a response to enhanced security measures against traditional identity theft. This type of fraud involves creating new identities by blending real and fabricated personal information, making detection difficult and posing unique challenges to card issuers.

Initially, synthetic identities were relatively rudimentary, but as technology advanced, so did the complexity and sophistication of these fake personas. Today, fraudsters employ machine learning algorithms and AI-generated profiles to create more convincing synthetic identities, enabling them to pass security checks and obtain credit cards.

Noteworthy emerging challenges:

- **Automation:** Fraudsters use automated tools and bots to quickly create and manage many synthetic identities, increasing their chances of success while reducing manual effort.

- **Collaboration:** Organized crime groups increasingly collaborate to share resources, expertise, and stolen data, making it easier for criminals to carry out large-scale, sophisticated synthetic identity fraud operations.
- **AI-generated profiles:** Artificial intelligence creates realistic, yet fake, online personas that give legitimacy to fraudulent applications and can evade detection systems.

4.8 Scams

Scams have been a persistent issue for the card-issuing industry since the inception of credit cards. Early scams involved simple schemes like stealing physical cards or using counterfeit cards to make unauthorized purchases. As technology progressed, scammers developed more sophisticated methods to defraud cardholders and issuers.

The advent of the internet dramatically changed the landscape of scams. Cybercriminals devised new tactics, such as phishing emails and fraudulent websites, to trick cardholders into disclosing sensitive information, enabling unauthorized transactions or account takeovers. The rise of e-commerce further exacerbated the issue, creating new opportunities for fraudsters to exploit.

With scams, the classic attacks are still highly effective (Phishing, Fake Advisor, Romance), but there are also emerging challenges. There are 100s of scam types that can vary and evolve over time.

Noteworthy challenges include

- **Tech support scams:** Scammers pose as representatives of well-known companies, offering assistance with nonexistent technical issues to gain access to victims' devices and card information.
- **Gift card scams:** Criminals exploit the popularity of gift cards by selling counterfeits or using social engineering to persuade victims to purchase gift cards and share the card codes, which are then used or sold for profit.
- **Cryptocurrency scams:** The rising popularity of cryptocurrencies has attracted scammers who devise schemes such as fake investment opportunities or phishing attacks targeting digital wallets.

4.9 Friendly Fraud (AKA Chargeback Fraud)

Friendly fraud (sometimes “chargeback fraud”) occurs when a legitimate cardholder disputes a transaction they knowingly authorized, often to avoid paying for the purchase or service.

In the early days of friendly fraud, card issuers tended to side with customers in disputes, increasing fraudulent claims. However, as friendly fraud became more prevalent, the industry recognized the need to address this issue to minimize financial losses and maintain merchant relationships.

This can be especially challenging to detect when a customer has recently signed up and the issuer has limited data or history about the user (e.g., identifying if they are a repeat offender). Card issuers are also impacted by liability. If the customer made a purchase and passed 3D secure (additional online security), the card issuer must cover all losses incurred by the merchant, even if they suspect fraud.

Noteworthy emerging challenges:

- **Normalizing friendly fraud:** The internet and social media have inadvertently normalized friendly fraud, such as sharing how to take advantage of chargeback rules. Opportunists discover that signing up for Fintech accounts is rapid and that they can quickly generate income from persistent friendly fraud.
- **Subscription services and recurring payments:** The rise of subscription services has increased friendly fraud, with cardholders disputing recurring charges they had initially authorized but later decided to avoid. Often this is simpler than canceling the subscription with the merchant.
- **Family fraud:** Family members, especially teenagers, may unknowingly contribute to friendly fraud by making unauthorized purchases, which the cardholder later disputes.

4.10 Rapid Account and Virtual Card Creation

Rapid digital onboarding (eKYC) and virtual card creation emerged as a response to the increasing demand for fast, convenient, and secure payment methods in the digital era. These technologies gained traction in the 2010s and have since transformed the card-issuing industry.

5.1 Leverage Device and Behavior across the customer lifecycle

Historically, the customer lifecycle has been too piecemeal.

Fraudsters are always on.

And fraud controls must be too.

Scam prevention example: During a scam, a customer might use a legitimate identity to send money to what they believe to be an investment opportunity or a romantic partner in distress. This customer passed KYC and authorized payment to the wallet or financial institutions. There is very little to suggest something fishy was happening.

If we focus on the device, we might see that the elderly customer had used remote screen-sharing software (often used by scammers to “assist” the elderly). If we focus on the user, we might see that they’re acting distressed compared to their usual activity.

If we combine the user and device signals with traditional methods like KYC and transaction monitoring, we might see that the user behaves strangely and that the transactions look odd. Not only that but the wallet or account they’re trying to send funds to had been seen before and was a known fraudster by another Fintech company or financial institution. Sardine might also have seen the device or user behavior before and assigned that device a negative risk score

Other examples of sophisticated device and behavior biometrics can detect

- **Card theft:** Detects when a card is being used in a different geolocation than a user's device.
- **Account takeover:** Detects when users behave differently in how they type, swipe or hold devices.

We can understand the victim and the fraudster by knowing users and their behaviors across devices.

5.2 Data Enrichment

If all fraud problems are data science problems, issuers need the broadest data set available within applicable law for fraud detection and prevention. This can include but is not limited to, bank transaction data, bank consortia data, email, Telco, and government data. It also often includes scanning the dark web for known breaches and high-risk credentials.

Examples of data enrichment can help detect:

- **Identity theft:** By identifying known stolen credentials from dark-web searches card issuers can reject or screen credentials that appear in these databases
- **Application fraud:** High-risk email or mobile numbers may include prepaid phone numbers or throw-away email addresses. This may be a signal of a higher-risk user.

5.3 Risk-based onboarding

Issuers can apply more friction if device, behavior, or data enrichment signals suggest the user could be high risk. This might include asking for more information from the user, pushing the application to manual review, or rejecting the application entirely. Conversely, if the device, behavior, and data show very low risk, the card issuer can remove steps from the standard onboarding process to increase conversion.

Risk-based onboarding can help deliver

- **Higher conversion for good users:** When data enrichment, device, and behavior signals do not show high risk, data can be auto-completed and entire onboarding steps removed.

- **Friendly fraud prevention:** Detect if the cardholder's relative is using a card instead of the cardholder – based on behavior signals on how someone holds the phone

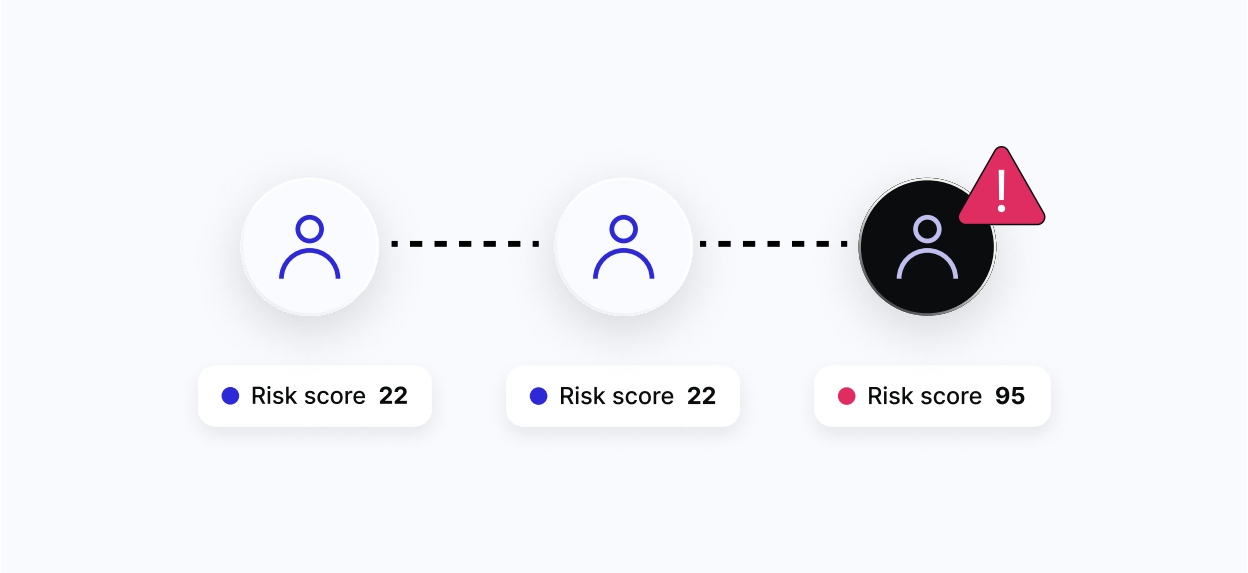
5.4 Rules built for card issuing use cases

Card issuers employ a series of rules to increase friction or even block transactions. There are countless examples, but consider value, volume, and velocity for simplicity. This could be high risk if a single device or mobile number has applied for 10 different accounts or is making 100s of tiny transactions. This control has existed for decades but constantly evolves as the threat model evolves.

Rules engines can help prevent

- **Rapid virtual card creation:** Detecting the speed of virtual card creation, or the velocity of cards created by the same device across different accounts, can flag help to screen against this emerging risk.
- **(CNP) Card not present fraud:** Fraud transaction amounts, times, and device geolocations can be consistent with friendly or 3rd party fraud patterns that can be screened with rules to detect those signals in combination.

5.5 Risk-based User Scoring throughout their lifecycle



Users display consistent behavior in transacting, using the device, and behaving. This pattern is unique to every user and can be measured with increasing confidence over time. If users suddenly deviate from their established patterns

- **Friendly fraud prevention:** Detect if the cardholder's relative is using a card instead of the cardholder – based on behavior signals on how someone holds the phone
- **Account takeover:** Detects when a user is behaving differently in how they type, swipe or hold devices.

5.6 Custom ML models and anomaly detection

One of the toughest challenges fraud operations teams faces is knowing what data to consider when evaluating risk. Data science and machine learning can help by flagging anomalies in transactions, devices, behavior or any other data element related to card issuers, merchants and cardholders.

- **Synthetic identify fraud:** When creating synthetic identities, fraudsters will behave in a way that is consistent to the individual or fraud ring. ML can help screen this behavior.
- **Card skimming/ shimming:** Advanced anomaly detection can identify potentially fraudulent merchants where a card skimmer may have been installed

6. Issuers lack an ideal solution to implement these controls and get the best performance

Not only are the fraud types continuing to evolve and become more complex, the skills and effort issuers need to keep pace with the fraudsters is exploding exponentially.

Ultimately all fraud problems are data science problems.

And often, fraud problems are really compliance and AML problems.

This creates a series of challenges for issuers to overcome.

1. If they build in-house they have to
    a. Recruit a world-class fraud ops and compliance team
    b. Recruit a world-class data science team
    c. Integrate up to 15 different vendors, many of whom don't share data
    d. Continue to invest in R&D for this team rather than as an operational function

2. If they outsource, they must
    a. Integrate up to 15 different vendors, many of whom don't share data
    b. Rely on the quality of vendor decision-making
    c. Manually work around gaps between fraud & compliance

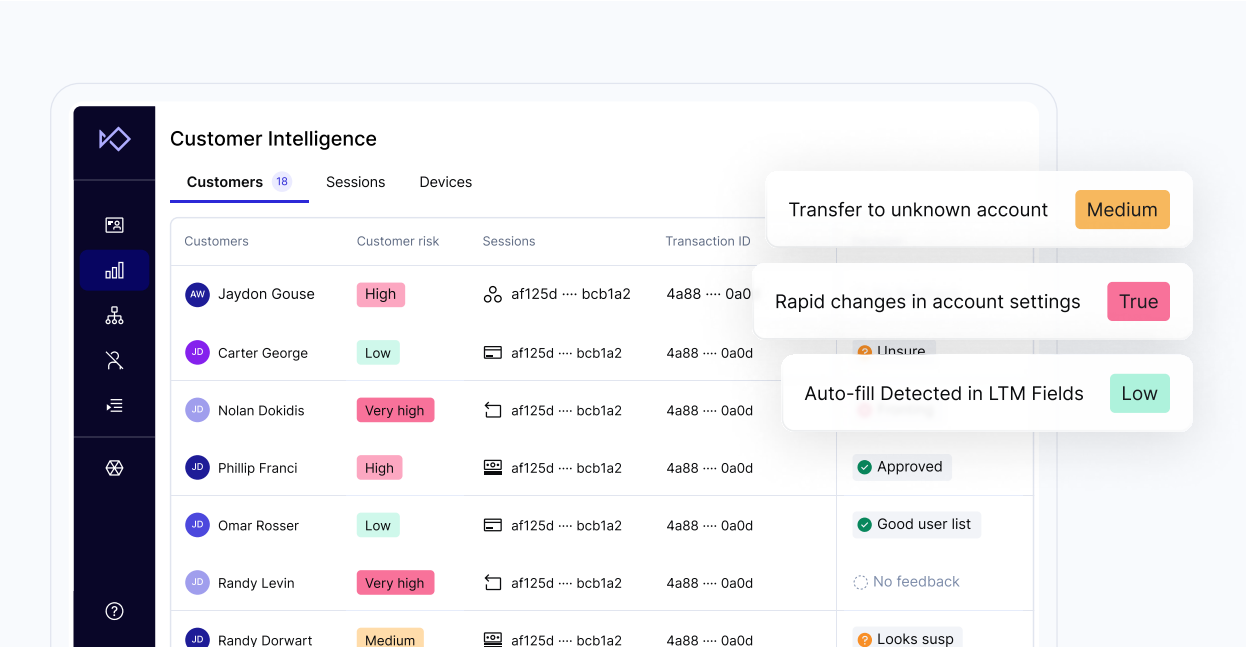
Specialist skill sets are hard to acquire and even harder to retain. Typically the fraud & compliance capabilities that are available by default from payments and BaaS providers are not tuned to the specific needs of a card issuer. To get the most of the products, issuers need a full-time staff focussed on identifying the specific fraud and compliance threats their business faces.

Historically issuers had to put together 10 to 15 different vendors, each with their own rules engine and many of whom didn't share underlying data and signals.

So issuers end up with a series of black box solutions, a patchwork of providers, and sub-optimal performance because none fits together. The fraud team can't flag things to compliance in a timely manner. The product team is battling to remove friction, while the fraud team potentially adds it.

None of this is ideal.

7. The Sardine solution moves faster than issuing fraud



Sardine is the only solution in the market for card issuers that can combine all of the key requirements card issuers have with one API, one dashboard, and one integration.

Issuers need

1. Balance and optimize fraud vs. friction for the highest conversion
2. Gain instant sophistication to avoid the new program avalanche of fraud
3. Consolidate all providers and integrations into a single hub that's "self-build" good
4. Combine fraud and compliance controls, processes, and data
5. Gain consistent R&D without more complex integrations
6. Have complete control of their data

7.1 Create the right friction at the right time with Step-Up verification

Sardine can invoke step-up verification throughout the customer lifecycle based on signals from the device, behavior, proprietary ML, and 30+ data providers. Sardine builds this into a consistent pattern we call the "same user score," allowing the platform to detect more account takeovers with fewer false positives.

One client reduced their false positives by nearly 3x in the first month of using Sardine to detect account takeover and reduced account takeover fraud by 38%.

The Sardine platform features:

- **Issuer push notifications:** Require step-up verification of a transaction from a user, or push into queues.
- **Multi-factor re-authentication:** Send users one-time passwords (OTPs), validate PII or KYC data, or require biometric inputs.
- **Customer Risk Score:** A risk weighting applied over time that Sardine's data science and ML models predict is a single human and their activity patterns. Sardine customers can track the customer risk score across the entire customer journey and be able to reference this score later in their internal business logic and Sardine rule engine executions

7.2. Become an instant specialist

At Sardine, we've combined the world's most experienced data science, ML, fraud, and compliance nerds into a single company. Consistently, we find we can improve performance on fraud detection and AML and reduce costs simultaneously.

It's an extreme example, but one client reduced their manual and human cost base by 10x by shifting to Sardine. That means more runway, more capital to invest in their core competencies, and better fraud protection.

The Sardine platform features:

- **1000s of Pre-built rules:** built for the most common fraud typologies that are trained on the highest-risk payment types
- **Cutting-edge data science and ML capabilities:** in the market to enhance and complement the rules-based system
- **A team of in-house specialists:** constantly evolving the rule sets and ML models and partnering with issuers to evolve controls to their internal OKRs and KPIs.

7.3. Get the flexibility of self-build with a single dashboard and integration

The Sardine platform requires card issues to integrate with just one API, one dashboard, and rules engine. Sardine clients consistently note that the flexibility is the best in the market because the platform features:

- **Single dashboard and rules engine:** Combine any data signal from any source, 3rd party or internal system to create sophisticated and dynamic rules. Push to production or use in “shadow” mode to validate rule performance before use.
- **30+ data providers & best in class partners:** Combine capabilities from the best eKYC, data, bank consortia, open banking, and more partners without the cost and complexity of orchestration or integration.
- **Ultra lightweight SDK and API:** Sub 100ms response times in real-world conditions from the API, sub 100kb SDK for devices

7.4 The single hub for Fraud & AML controls

Sardine comes preconfigured with 100s of the most common typologies pre-created and available the moment you sign & integrate. Including

- **AML, Sanctions, PEPs & Transaction monitoring:** The Sardine platform, dashboard, machine learning, and rules engine are all applied to AML typologies. This works across fraud and compliance, allowing fraud patterns to be built into AML cases by analysts.
- **Case Management:** Sardine allows for cases that are triggered by a rule to be queued into a case management system, whereby they can be assigned to an analyst, who can approve/decline a case; leave detailed notes, including attach supporting documentation to the case; and once reviewed, they can reassign it to their manager.
- **Sardine Network Graph:** Sardine provides a network graph visualization tool that allows an analyst to identify users connected via shared devices or shared addresses. Then an analyst can review alerts for this cluster in totality instead of individually.

7.5 Consistent, Rapid R&D without complex integrations

A core value at Sardine is speed. Not just moving faster than fraudsters but in feature velocity, rule creation, and going the extra distance to deliver the best performance in the market.

- **Data science driven:** The Sardine DNA is in cutting-edge data science, mixed with an in-house fraud and compliance operations team. This unique specialism allows Sardine to deliver what card issuers would if they had the budget and priority internally.
- **Anomaly detection:** Sardine machine learning algorithms and anomaly detection engine trigger alerts to a joint slack channel, and customer queue, and the alerts are also available in the dashboard.
- **Rapidly evolving roadmap:** Sardine's product consistently evolves based on customer feedback, evolving fraud patterns, and Sardine's own operating experience

7.6 Open data architecture

For some customers, we're their entire risk stack; for others, just a small piece.

Sardine is an API-first platform. And we provide access to all the rich device and behavior data and all our machine-learning features in our API response. Want to feed your ML models with Sardine data? You got it. Want to import things into our rules engine? You got it.Want to do one but not the other? You got it. Want to do both? Of course you can.

- **Open data:** The Sardine customer API will return any data relevant to a transaction or interaction (including from any 3rd party data enrichment providers)
- **Open signals:** The Sardine device and behavior signals are fully available and fine-grained.
- **Open model responses and rule performance:** Crucially, Sardine shares how it got to a risk score, from the model's output to the rules that fired.

For some clients, we also expose the machine learning features directly.

7.7 The fraud team you hire as an API

With premium support, Sardine offers a dedicated team of strategic account managers & risk analysts who work with your compliance team to create new rules and monitor activity as needed.

8. Learn more about Sardine

One client reduced manual work and overhead by 10x and false positives by 80% within 3 months of integration. Sardine also reduced card fraud by 80%, saving $1.3m for one of the world's largest Crypto exchanges

The key question is, can you afford not to work with Sardine?

If you want to go deeper

- Check out our overview of Device Intelligence and Behavior Biometrics
- Connect with us on LinkedIn & Twitter
- Or email us your biggest card issuing fraud challenge to hello@sardine.ai