Global business trends:

Protecting growth ambitions against rising fraud threats

For permissions, write to us at the address below
Experian
Cardinal Place
80 Victoria Street
London
SW1E 5JL
United Kingdom

T +44 (0) 20 304 24200
F +44 (0) 20 304 24250

Table of contents

Foreword

We've long accepted that fraud loss is a cost of doing business. But something has changed. Fraudsters have evolved — they leverage technology and sophisticated underground networks — and actual losses now exceed expected losses. In an effort to patch the holes and plug the gaps, fraud prevention has become overly complex and is negatively impacting the customer experience. I think we can all agree the status quo is no longer effective.

Fraudsters are relentless, but they are no more determined than you are. They count on vulnerabilities that you can eliminate. They expect to be chased, not outmanoeuvred. Companies need to be as forward-looking in fighting fraud as they are in growing revenue and attracting new customers. It's time to move beyond one-size-fits-all fraud strategies and instead deploy right-sized solutions so that the appropriate level of protection is applied to every single transaction for increased confidence and effortless customer interactions.

The reality of today's economy demands this change. Business is global – it happens 24 hours a day across countless digital and face-to-face settings. Creating a secure, streamlined customer experience is paramount. Although once considered separate mandates managed by separate teams, revenue generation and fraud prevention are now intrinsically linked. Siloed ways of working are no longer viable. In my experience, and in conversations I've had with organisations of all shapes and sizes, this has become clear: the more closely aligned your product development, marketing, customer experience and fraud risk strategies, the more successful the business. Modern fraud mitigation approaches make it possible for fraud prevention to play an active role in driving growth and a positive customer experience.

Experian understands these dynamics, and we're helping the marketplace fully realise growth ambitions without being constrained by intrusive fraud controls. This report highlights five global trends for business executives to understand when developing modern fraud mitigation strategies. We look forward to continuing this conversation with you.

Steve Platt
Executive Vice President
Fraud and Identity,
Analytics and Decisioning Software

Five trends for modern fraud strategies

Experian believes in a forward-looking way for businesses to approach fraud mitigation – one that will mitigate financial loss, enrich consumer relationships and drive growth. Whilst most of the industry is talking about how fraudsters are circumventing current fraud detection systems and how businesses should fortify themselves against these vulnerabilities, this tactical approach will not outpace the fraud. That's why we approached this report differently. We've created it with senior business executives and fraud professionals in mind, offering new insights for how the alignment of strategies, teams and processes can protect growth ambitions from rising fraud threats.

There are five global trends in modern fraud mitigation strategies:

1 Applying right-sized fraud solutions to reduce unnecessary customer disruption and manage risk

Fraudsters hide in plain sight, blending in with legitimate customer traffic — which is why companies accept a certain amount of customer disruption as an undesirable but necessary part of catching fraudsters. The level of this disruption is wildly out of balance, however. The ratio of disrupted legitimate traffic to actual fraud attempts is now as high as 30 to 1. In other words, 30 legitimate customers are challenged or blocked — for reasons they rarely understand — in order to catch one fraudster. As more purchases (and, therefore, more fraud attempts) move to the online channel, the rate of challenges to legitimate transactions will only increase. The net result is a consumer population irritated by the unending number of challenges to their online activity, as opposed to just a few years ago when consumers welcomed banks and finance companies protecting customers from the "bad guys."

To reduce customer disruption and appropriately manage fraud risk, companies need to apply fraud mitigation strategies that reflect the value and level of confidence needed for each transaction. We call this right-sizing the fraud solution. This approach, when aligned with your company's fraud rates and commercial strategy, increases the likelihood of catching fraudsters without disrupting the business of (and relationships with) legitimate customers. For example, if actual fraud attacks represent 1 to 2 percent of transactions, right-sized solutions should identify no more than 4 to 6 percent of transactions as probable fraud.

> **Experian helps its 10 largest clients to detect and prevent fraud worth $500 million each year, maximising profitability whilst at the same time providing secure, hassle-free customer interactions**

2 Having a universal view of the consumer is the core of modern fraud mitigation and marketing

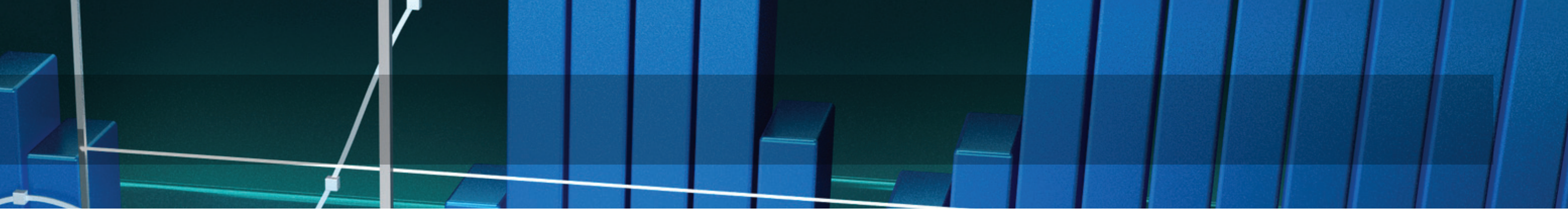
Companies try to reduce the anonymity of the online world by verifying customers primarily through identity challenge techniques (i.e., challenge-response questions), but the harsh reality is that most identity data has been compromised. In the past two years alone, more than 2.2 billion personal records have been exposed as the result of data breaches[1]. According to Javelin, one in five data breach victims suffered fraud in 2015, a rise from one in seven in 2014[2]. A multi-layered approach to authentication is considered the gold standard for identifying legitimate customers, but this can be hard to do without creating so many challenges that the customer experience is adversely affected.

Knowing the individual customer extends beyond a traditional 360-degree view. It means having knowledge of a person's offline and online behaviour, not only with your business, but also with other businesses with which that customer has a relationship. This information isn't "owned" by a single organisation. It requires a more expansive view and collaboration across teams within a company, businesses within an industry, and across different industries. Applying the insights from information such as online behaviour, historical transactions, identity, biometrics, and device intelligence gives companies a more expansive view. It means truly being able to know and recognise your customer, and making their interactions with your business relevant every time.

Having access and insight into this **universal** consumer behaviour, down to the transaction level, will be necessary for fraud mitigation in the future. The ability to know and recognise a legitimate customer will make fraudsters easier to differentiate. This will mean fewer unnecessary and aggravating challenges to customers — frictionless is the future. It will also help achieve higher conversion rates for marketing campaigns and improve marketing return on investment by delivering the right message to the right person when they are most receptive to it and in the most convenient channel. Taken together, this is a clear example of the benefits of converging mandates around business growth and fraud mitigation.

[1] Experian data on file

[2] Javelin 2016 Identity Fraud: *Fraud Hits and Inflection Point*, February 2016



3 Expanding your customer view through a blended ecosystem

Many organisations have launched projects to achieve a single customer view: collaborating across internal silos to bring together information about their customers and their interactions. Whilst they're good in theory, the conflicting priorities of internal silos turn these projects into multi-year undertakings that are challenging and costly. Even if attained, a company's single-customer view may still achieve only a partial view of the consumer. This is because their view is solely based on their relationship with a consumer, rather than the consumer's relationship with other companies. Fraudsters on the other hand have this broader view, and they use it to their advantage.

The volume of compromised data and ever-changing fraud schemes has created a threat landscape that can no longer be managed in a siloed manner. Increasingly, companies are participating in a blended ecosystem — working with vendors, customers, partners and even competitors — that can bridge disparate data and internal siloes. The end result is an enhanced customer experience that supports business growth, without sacrificing protection.

4 Achieving agility and scale using service-based models

Fraudsters act fast, and companies must at least keep pace (and preferably be a step ahead). To spot the latest fraud attacks, many large institutions employ statisticians and modellers to monitor and develop rules based on different combinations of variables. These complex fraud risk models require a lot of time and investment to set up and maintain and, therefore, a significant business case is needed to gain approval to proceed. Once approved, it takes time – often months – to analyse, build and deploy the models. It's only at that point that companies can respond to the threat, but by then it's likely that fraudsters have done damage.

Fraud adapts quickly, and when you're too slow to respond to threats, it can come at great expense to your business and customers. Your systems and business processes become a source of vulnerability — which is why more companies are turning to service-based models that provide greater agility and faster response to emerging threats. Service-based fraud models give you the benefit of highly skilled expert analysis, analysis that is regularly updated to respond to fraud trends or incidents seen across the industry at any given time, often protecting you before the fraud happens. These service-based fraud models also adapt and scale to support your business, no matter how fast your volume grows or which products, channels or geographies you pursue.

5 Future-proofing fraud solution choices

Companies need to be as nimble as fraudsters, with fast access to the right tools and data whenever they need it. But that's often not the case, leaving companies in the wake of evolving fraud schemes. The current approach of adding new tools on top of existing solutions is creating complexity that is becoming expensive to integrate and difficult to manage. You need flexibility and scale, to get more out of what you have in place, test strategies and utilise new technology. You need a way to connect the best solutions available and access a range of data sources to keep up with the speed of fraud.

At Experian, we understand these needs and developed the first smart plug-and-play platform that allows you to connect to your own solutions, Experian products, and third-party vendors together in one place to better protect customers from fraud threats. It's called CrossCore™ — and it's making the industry's fraud and identity solutions work better for everyone.

Throughout this report, we discuss how these five trends will fundamentally change the dynamics between companies and fraudsters. Armed with greater knowledge and agility, companies will become a much tougher target for fraud. Whilst fraudsters will encounter more obstacles to thwart them, customers will encounter fewer challenges to protect them. Having greater knowledge and agility will require an expanded view about the consumer, further underscoring the essential collaboration between the product development, marketing, fraud teams and third parties — a collaboration driven by the shared goal of growing a sustainable business and protecting its ambitions against rising fraud threats.

Growth requires stronger relationships

Business growth depends on opening new channels, expanding offerings, and extending into new geographies and markets — all whilst maintaining a positive customer experience that is relevant and consistent. Without this, it is hard to build strong relationships with your customers and create brand loyalty.

Typically, product and marketing teams (who generate business demand) view fraud teams (who minimise financial loss) as a block to their efforts. They see fraud teams as creating unnecessary obstacles and points of friction that can result in lost business. This is a legitimate concern given fraud strategies in the past have been overly aggressive, or did not match the nature of the transactions. Here are a few examples of how this has happened:

For example:

- Adding more security challenges for different products or channels undermines a seamless customer experience by creating new hoops for customers to jump through and more processes for them to follow. Customers simply do not understand why security for an existing relationship with your product or service can't be automatically extended to new products and channels.
- Declining transactions in order to prevent possible fraud often results in customers using other credit cards at the point of sale; this may be a temporary inconvenience, or it may mean that you lose your coveted "top-of-wallet" position.
- Putting longer hold times on transactions in order to confirm legitimate transactions can result in financial difficulties for customers; customers today have a lower threshold for inconvenience and a greater willingness to change providers, so these kinds of fraud measures can lead to customer defection.

Given this context, relationships are often strained between teams on the product and marketing side and their colleagues in fraud prevention. Unfortunately, this benefits the fraudster, who counts on organisational siloes to exploit blind spots and evade detection.

Best practices for aligning revenue goals and fraud mitigation

Experian recommends three organisational best practices that are fundamental for aligning revenue goals and combating fraud. The good news is that *none of these require changes in reporting structures or functions.*

- **Regular, proactive communication** across product, marketing and fraud teams to help anticipate new points of attack. For example, including fraud teams in discussions about new product development, channels, markets and promotions can help uncover new opportunities beyond just catching fraud.
- **Common goals** for optimal customer experience across product, marketing and fraud teams to encourage a more collaborative way of creating targeted growth and fraud strategies. For example, sharing information about your customer's behaviour to help improve offer redemption and fraud detection.
- **Rethink how customers interact** with your business, moving away from isolated interactions to a lifecycle relationship mentality. For example, shared responsibility for fraud across account opening, access and transactions will help detect fraud earlier and prevent financial loss.

The impact of these three best practices is seen in the collaborative way in which internal teams will share information.

> "We've seen a change over the last 5 or 6 years – businesses are recognising that creating a positive customer experience whilst protecting the consumer and the organisation can be a differentiator"
>
> — Adam Fingersh, General Manager, Fraud and Identity Solutions, Experian

Knowing your customers' behaviour creates more targeted fraud strategies

In the past, marketing and sales teams were seen as the collectors and custodians of information about the customer. Fraud teams also have access to a tremendous amount of data about customers, but this information is used primarily to differentiate actual customers from fraudsters. Adding marketing insights around consumer behaviour to fraud strategies will not only create more targeted, effective strategies, but will also help marketing teams plan, segment and deliver products and offers with greater success.

From isolated interactions to lifecycle relationships

In addition to better cross-functional sharing of information, greater collaboration is needed across teams and processes that are highly susceptible to fraud – account opening, account access and maintenance, and transactions. Different internal teams are responsible for each of these processes, and these teams operate independently of one another, often with varied solutions and different risk mitigation philosophies. Whilst this is a simplified depiction of business processes, things get more complicated when you look across multiple product types, channels and geographic regions.

Putting the customer at the heart of your business helps you to rethink your business processes in terms of a customer engagement lifecycle. Adopting this holistic approach encourages the sharing of information across the business processes, which helps to proactively detect fraud earlier at the point of account opening or account access and maintenance, and reduces the vulnerability of financial loss later at the point of transaction. Sharing customer information across the processes within the lifecycle can reduce customer friction caused by continuously verifying routine account activities, and save on capital and operational expenses caused by increased fraud investigations.

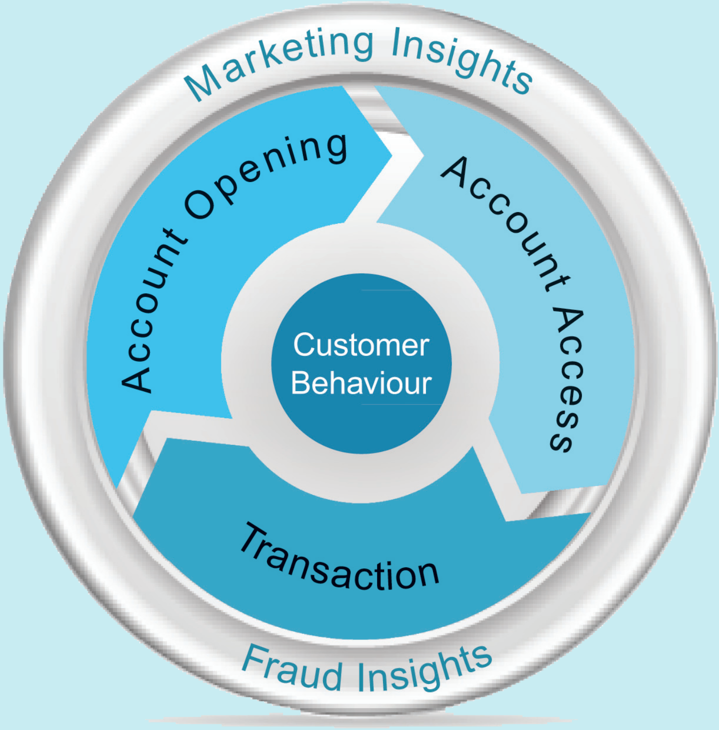


Figure 1: Moving from isolated to lifecycle relationships

Account opening

> “The conversation is changing. In addition to risk tolerance, executives and fraud strategists will talk about customer disruption tolerance.”
>
> — Matthew Lane, Global Fraud and Identity Service and Operations, Experian

The Association of Certified Fraud Examiners (ACFE) devotes considerable time to the problem of account opening fraud in its publication Financial Institutions Fraud. It notes that “a majority of institutions are reluctant to develop strict fraud prevention policies because determining the costs and benefits of prevention are almost impossible.” It adds: “Even if an account was opened fraudulently, until money is lost due to deception, there is no way of showing that the account would have lost money.”

Based on our experience working with large and small financial institutions and merchants globally, we have seen a much broader spectrum of responses. Companies may block or delay transactions, flag suspicious accounts and suspend accounts after seeing a suspicious point-of-sale transaction, or block accounts and issue new cards before a point-of-sale transaction. The type of responses can vary widely and generally based on a combination of their organisation’s size, tolerance for risk, available investigators, level of system automation, and access to information.

Why “strict” is not a useful characterisation for fraud policies

Given the broad spectrum of responses, the term “strict” doesn’t serve as a relevant way to characterise fraud strategies.

If you do not factor in the importance of the customer experience, then the more aggressive the fraud mitigation measures, the better. But that is not the direction in which the industry is heading. Draconian measures are out of step with maintaining the seamless customer experience that consumers expect. In fact, with rare exceptions, our clients view a positive customer experience as integral to business growth.

That said, many organisations view a positive balance between risk mitigation and an ideal consumer experience as unattainable. We believe that it is not just a question of balance, as though it were a tug of war with the customer in the middle.

The relationship between the two mandates is so important that each can improve and strengthen the other — an essential combination for sustainable business growth.

Whilst organisations like the ACFE are focused only on financial cost impact, Experian believes that conversation is expanding. That broader conversation will encompass the impact of fraud strategies on the customer experience, which is all about financial stability and growth for the business.

Fraud strategies, like business innovation, require agility and speed

When leading smartphone companies announced new payment options using mobile wallets, it created a tremendous amount of excitement. After all, about 30% of all online transactions during last year’s holiday peak were made using a mobile device.

There was little concern about fraud. Smartphones themselves employ strong anti-theft technologies (e.g. fingerprinting) and anti-fraud technologies such as tokenisation, which translates credit card number into an identifier that is useless for fraud purposes. With tokenisation, credit card information no longer has to be downloaded onto a merchant’s servers, removing the risk of data theft.

Did this neutralise the fraud threat, as everyone thought? Not at all. Fraudsters took note of the strong fraud measures at the front door and found a back-door vulnerability instead. They moved their attack upstream to the account opening and provisioning process, adding stolen credit cards to the mobile wallets. It took several months for the industry to catch on to the fraud — in large part because there was limited information sharing and no shared visibility between smartphone providers, card associations, and financial institutions.

The financial impact associated with adding unauthorised cards to mobile wallets has been relatively low, but the success rate has been higher compared to card-present frauds. This illustrates how fraudsters can capitalise on both unknown vulnerabilities in innovative offerings and blind spots between siloed functions.

Updated fraud models for account opening were simply not ready for the mobile wallet trend. That is not a reflection on in-house resources — it is simply the reality of how the pace of innovation can create exploitable gaps. Regression testing along with existing fraud processes can take weeks or months. Competitive companies do not want to delay the launch of a lucrative new offering like mobile wallets just so that fraud measures can catch up.

30% **of all online transactions during last year’s holiday peak were made using a mobile device**

Business application: Right-sizing fraud solutions

Most financial institutions have to cast a relatively large net to catch fraudsters. This is because fraudsters are hard to find in the crowd, so essentially the whole crowd has to be viewed with suspicion. Steps taken to block fraudsters often end up inconveniencing a disproportionate number of legitimate customers.

Modern fraud strategies necessitate applying the right level of confidence so that you're most likely to catch fraudsters without disrupting the business of (and relationships with) legitimate customers. We call this "right-sizing" the fraud solution. The table below illustrates how dramatically you can improve your fraud detection rate whilst reducing the number of false positives (which translates to less disruption for legitimate customers).

Key performance indicators for fraud teams	Industry average[3]	Experian fraud solutions[4]	Impact of right-sized fraud solutions on account opening
Manual review rate	15%	7.68%	Reduce manual reviews by 49%
Fraud rate	4%	0.46%	Reduce missed fraud by 88%
Fraud detection rate	50%	88.84%	Increase fraud detection by 78%
Attack rate	8%	4.18%	Reduce fraudulent attempts by 48%
False positive ratio	4:1	2:1	Reduce false positives by 50%

Table 1. Right-sizing fraud solutions for account opening. A right-sized approach means tackling the problem with a highly tailored solution that enables the business rather than crippling it. Two characteristics of this approach are: 1) understanding your attack rate, or how much and where the fraud is coming from; and 2) weighing the risk against the value of the transaction.

Mobile interactions will challenge — and assist — modern fraud mitigation

The expanded interactivity between businesses and consumers is seen through the growth of "mobile everything." Mobile is the anytime-anywhere access consumers have to your business, from making payments to the information stored on their device. These valuable customer interactions with your business are also opening up new opportunities for fraudsters.

Vulnerabilities in mobile wallets were revealed when fraud moved from transactions being made using a device to provisioning and enrolling a stolen credit card into a mobile wallet. The lack of integration across players in the ecosystem exposed gaping holes in front end security – making it difficult to verify that the person registering their card to the wallet was, in fact, the legitimate owner of that card. This exemplified how fraud moved earlier in the customer lifecycle – from transactions to account opening or account access and maintenance – under the guise of a secure technology.

More and more providers are offering to keep information stored in a mobile wallet further underscoring the importance of the trends mentioned in this report: right-sizing fraud solutions, achieving a universal view of customer behaviour, and leveraging relationships in the blended ecosystem.

[3] Experian estimates the industry averages based on a number of inputs. This includes tracking key indicators from sources such as consultants, analysts and other vendors, as well as factoring in publicly reported information related to security spend, customer friction and volume.

[4] Average results based on our client base

Account access and maintenance

Once an account has been created, customers want an easy way to access and maintain their account. This is where fraudsters spend most of their time, gaining access to customer information and making changes to accounts that often go unnoticed. Authentication measures are commonly applied at this customer interaction, but lack the sophistication to detect unauthorised activities.

Catch fraud earlier in the lifecycle

An attempt to commit transaction fraud can precede actual fraud by days, weeks or even months. In fact, unauthorised user activity (i.e. changing contact details or setting up mule accounts) is often the preparation fraudsters need for the ultimate action, which is to move money. These activities can be stopped at the account access and maintenance stage. But, at the stage where money changes hands — where there may be only seconds to detect fraud — it is more difficult to mitigate the risk quickly.

Many banks rely on transaction anomaly systems to execute a transaction request – completing a risk assessment in milliseconds, and usually with limited information. Fraudsters count on missed signals or gaps during this small window of time in which companies must analyse and approve transactions. Moving fraud detection earlier in the customer engagement lifecycle – from the transaction stage to the account access and maintenance stage – can dramatically shorten the time-to-detection and reduce the fraud loss rate by up to 60 percent[5].

Why multi-factor authentication is not optimal for the future

At one time, a user name and password was the gold standard to authenticate a customer and grant access to their account. Research shows that the average U.S. consumer has 25 online accounts, but only uses five or six passwords[6]. Experian has found that millennials have upwards of 100 online accounts with the same small set of passwords across those logins. These online accounts range from high-security environments to websites with virtually no security, like blogging sites. The fraudster simply has to find the password for the weakest sites, and then test the password in more fortified accounts, like your bank account.

In 2011, federal standards groups provided recommendations for layered or multi-factor authentication, such as adding biometrics or a one-time passcode. Multi-factor authentication is certainly stronger than single-factor, but it's still not the best approach for the future.

The fraudster knows what you are looking for

Organisations draw from a collection of possible multi-factor authentication challenges to define a specific sequence of challenges for a specific customer interaction. Once an organisation has set a sequence, it's just a matter of time before a fraudster can uncover one or more of the factors that make up that the sequence. In other words, you have just defined the parameters that the fraudster must focus on in order to be successful.

Let's look at an example of an organisation employing multi-factor authentication using a one-time passcode delivered to a customer's mobile phone. Knowing this organisation's set of challenges, the fraudster can log into the customer's mobile account through the cellular provider's browser application and intercept the text message, stealing the secure key before it's delivered to the customer's cell phone.

> "Moving fraud mitigation earlier whenever possible is one of the most valuable outcomes of taking a lifecycle approach. It proves more successful, less disruptive to the customer experience, and more cost-effective."
>
> — Mike Gross, Director of Product Management, Global Fraud and Identity, Experian

[5] Experian data on file

[6] TechRadar, July 2012

There is too much customer friction in a multi-channel world

Most companies offer consumers the opportunity to access accounts via multiple avenues, including Web, mobile, in-store and call centre. Whilst convenient for consumers, the challenge for businesses is incorporating multi-factor authentication in a way that is seamless for customers, when visibility across channels is low and risk management approaches are often inconsistent.

Less challenges means less friction for customers. And modern fraud strategies allow you to reduce those challenges without assuming more risk. Here are some approaches to consider.

1. **Authenticate based on fewer challenges:** The less fraudsters know how you recognise your customer, the better. Gleaning insights from data not visible to fraudsters – or even the customers themselves – can be used to know your customer without questions or passwords. These insights are from previous customer interactions across your products, teams and processes. Only you have access to this information and using it to authenticate customers improves their overall experience.

2. **Analyse patterns of behaviour:** You can quickly recognise your customers by looking at individual customer behaviour patterns and the devices used to access their accounts. You can also quickly flag suspicious attributes. For example, if a country of origin is incongruent with a customer's typical behaviour, you can know with greater confidence that fraudulent activity is taking place and flag it for investigation.

3. **Look at the universal consumer:** Having a universal view of the consumer can make it easier to recognise legitimate customers without challenging the customer or revealing your tactics to the fraudster. For example, you might use historical data on the customer to determine that they are logged in from the same handheld or laptop device they used to open the account three years ago, and that they've only used a handful of devices since that time to conduct transactions with other institutions and merchants.

> "Having visibility to accounts and transactions requires the ability to gain insights from information across channels, and even beyond your institution and your industry. This is where the blended ecosystem becomes a necessary part of your universal view and customer profiling."
>
> — David Britton, Vice President of Industry Solutions, Global Fraud & ID, Experian

Business Application: How loyalty programme fraud exploits vulnerability

Loyalty programme fraud is a prime example of how fraudsters can perpetrate lucrative crimes — and damage customer relationships — without ever exchanging actual money.

For years, loyalty programmes were most common in the travel industry. Now these programmes have become popular with restaurants, coffee houses, movie theatres, retailers and even your local pharmacy. This is creating a larger, more attractive market for criminals to target.

Companies create loyalty programmes to turn casual customers into repeat customers and ongoing customers into bigger purchasers. Customers take this relationship seriously and personally — which is why companies should not be surprised that customers react to loyalty programme fraud with particularly strong outrage.

In addition, the financial impact of a compromised loyalty account does not end when the fraudster steals or redeems all of the points in an account. As demonstrated in Figure 2 below, research shows that 26 percent of customers will cancel their rewards membership. About 17 percent will stop doing business with the company. And 37 percent will tell others about their loss and the vulnerability of the loyalty programme.

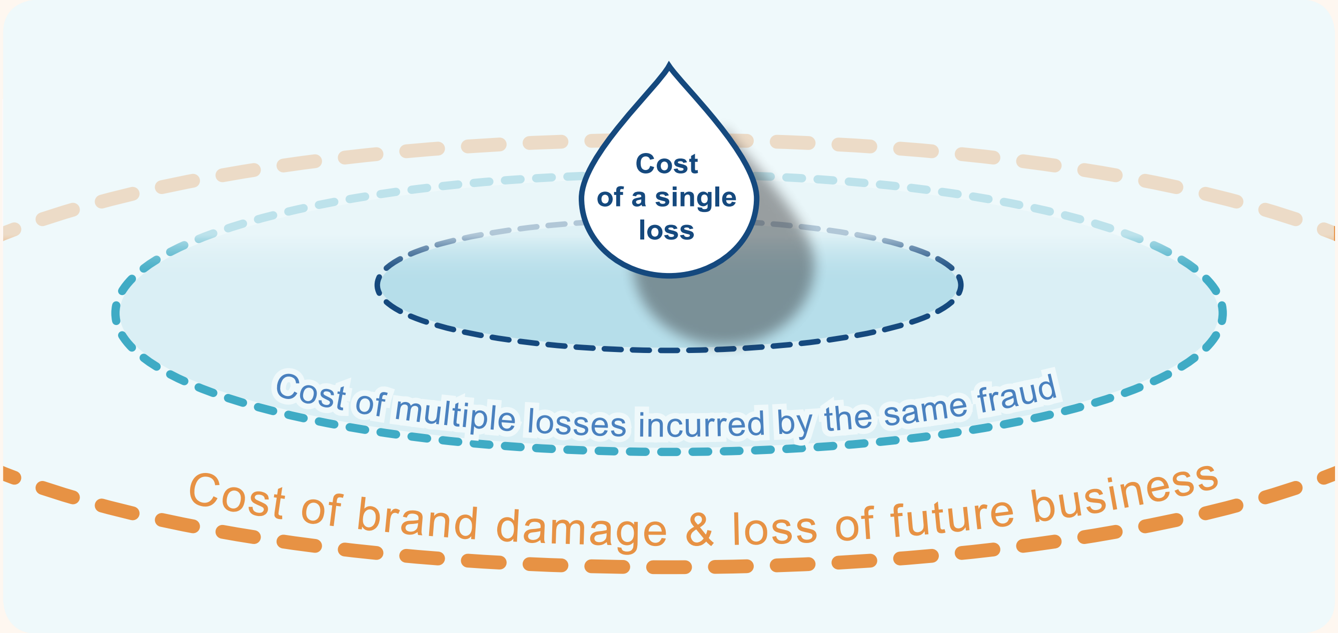

Cost of a single loss
Cost of multiple losses incurred by the same fraud
Cost of brand damage & loss of future business

Figure 2. Hidden costs of fraud. The financial impact of a compromised loyalty account does not end when the fraudster steals or redeems all of the points in an account, and can potentially have a greater impact on brand reputation and future business.

[7] Connexions Loyalty. Loyalty Program Fraud Report

Nearly three-fourths of loyalty programme managers report experiencing fraud attacks[7]. There are many reasons why this fraud is gaining ground.

Loyalty accounts are often not well-monitored nor protected

- Customers who join these programmes do not typically monitor their reward points with the same frequency as they do their bank accounts or credit card statements, so missing points may go unnoticed for months.
- Companies don't appear to be monitoring these programmes for fraud to the same degree as they monitor for other types of fraud.

Flexible (and exploitable) redemption practices

Many companies give customers a lot of flexibility in how loyalty points are redeemed. They recognise that customers appreciate having more choices in how they use loyalty points — cash, gift cards, purchases from an online catalogue and so on. Choice breeds complexity.

Fraudsters benefit from this complexity, however. Loyalty fraud attacks include the theft of loyalty points, the use of stolen points to make purchases that do not follow the traditional payment flow, and even reselling gift cards for cash (which provides a tidy way to launder money).

The customer's link to multiple loyalty accounts provides a roadmap for fraudsters

There is also a cascading effect that extends beyond a single company's loss. Someone who has one loyalty programme tends to have several — in the United States, the average consumer is a member of 29 programmes[8]. These programmes tend to have weaker security and require weaker passwords, which can lead a fraudster to infiltrate not just one but multiple accounts successfully, using the customer's compromised information gained from each account. Furthermore, if the loyalty account that the fraudster finds initially is not attached to a credit card, following the trail to other accounts may ultimately lead to one that is linked. At this point, the damage can escalate from point redemption to compromised credit cards or bank accounts.

Loyalty programme fraud is a type of account takeover that the fraudster perpetrates during the account access and maintenance part of the lifecycle. Can you find more fraud today without adding customer friction?

Our customer data says: definitely.

Key performance indicators for fraud teams	Industry average[9]	Experian fraud solutions[10]	Impact of right-sized fraud solutions for account takeover
Manual review rate	0.10%	0.01%	Reduce manual reviews by 90%
Fraud rate	0.001%	0.0004%	Reduce missed fraud by 60%
Fraud detection rate	33%	68%	Increase fraud detection by 2.1x
Attack rate	0.003%	0.001%	Reduce fraudulent attempts by 67%
False positive ratio	99:1	9:1	Reduce false positives by 91%

Table 2. Right-sizing fraud solutions for account takeover. A right-sized approach means tackling the problem with a highly tailored solution that enables the business rather than crippling it. Two characteristics of this approach are: 1) understanding your attack rate, or how much and where the fraud is coming from; and 2) weighing the risk against the value of the transaction.

[8] Connexions Loyalty, Loyalty Program Fraud Report

[9] Experian estimates the industry averages based on a number of inputs. This includes tracking key indicators from sources such as consultants, analysts and other vendors, as well as factoring in publicly reported information related to security spend, customer friction and volume

[10] Average results based on our client base

Transactions

Don’t chase the money if you can detect it earlier

Many companies feel that protecting transactions is the most important area to which to shift their focus after the account opening stage. Transactions certainly should be considered, but one of the other benefits of looking at account activity (or non-monetary transactions) is that you’re stopping the emerging threat earlier and not chasing money after the transaction.

Chasing fraud post-transaction traditionally required a heavy operational expense. It is a labour-intensive process, requiring skilled investigators who can make split-second judgments about transaction legitimacy. Because investigators have to look through such a high volume of transactions, they may err on the side of blocking transactions automatically to give them more time to investigate.

Even investigations can be thwarted by fraudsters. They can forward phone numbers (via telecommunications and cell providers). They can change the numbers associated with an account earlier in the lifecycle and let that sit for 45 days so it looks like an established number on the account. When an investigator calls later to verify a transaction, they are calling the fraudster, not the actual customer.

Stopping fraud frees up valuable resources

Having an accurate initial filter is critical to achieving more efficient, more effective and less costly fraud mitigation downstream. You can apply investments (especially skilled investigators) in downstream resources to review more sophisticated cases and perform rich link analysis. Rather than working the events in the queue sequentially, investigators can start looking at collective events and events across boundaries and relationships.

This also drives toward a right-sized fraud approach. The benefit is that hundreds of investigators are no longer spending time reviewing a high volume of false positive transactions to try to identify a small number of fraudsters.

Right-sizing fraud solutions and strengthening fraud measures earlier in the lifecycle of customer interactions is even more applicable to e-commerce vendors. Loyal customers can make purchases without logging into their accounts, so there is no profile information with which investigators at the transaction stage can quickly ascertain whether the charge or purchase is legitimate.

> “Leveraging a layered approach, you can provide a frictionless customer interaction, and recognise those individuals coming into your site, your store, your call center, or applying for a loan that may be fraudulent.”
>
> — Gary McVie, Director Global Fraud & ID, Experian

Business application: Increase in card-not-present transactions requires agility

Card-not-present transactions are highly susceptible to fraud. This broad, ever-expanding category includes mobile wallets, digital wallets and online payments using a credit card. What they all have in common is that the transactions are completely anonymous (requiring no face-to-face interaction with the customer).

In the drive to own as much of the consumer’s business as possible, companies are delivering a near-constant stream of innovative products and services. The inspiration for a large portion of these innovations is creating a seamless, convenient way for consumers to transact business, including:

- Starting a transaction on one device and finishing it on another.
- Enabling more ways of shopping and doing business on a single device.
- Storing personal and payment information on a site (card on file) to make future transactions faster and easier.

The mobile wallet is just one of the innovations that have challenged fraud detection at the point of transaction. When you consider all of the emerging card-not-present scenarios, it is clear that fraud teams will need to be a lot more agile in order to adapt and respond. The following are some of the changing and challenging dynamics of card-not-present transactions:

- Consumers are likely to adopt mobile wallet payments at a faster rate if EMV chip readers aren’t widely available.
- Consumers may use physical cards longer if mobile wallets are not accepted or are too difficult to use at common retailers such as gas stations, grocery chains, supermarkets and convenience stores.
- Consumers may value payment methods associated with loyalty rewards even above convenience.
- Consumers are likely to start adopting alternative payment methods using new types of devices, like wearables, as the Internet of Things (IoT) continues to increase.
- Consumers are increasingly likely to use their mobile phones to conduct more financial transactions; for the unbanked consumer population, this means unprecedented access to products and services.

Emerging trends

Machine learning is a powerful predictor of fraud, but is not a panacea

Machine learning has become an invaluable tool in the fight against fraud. It combines computational statistics, artificial intelligence, signal processing, optimisation, and other methods to identify patterns. Machine learning has been a significant breakthrough in helping companies move from reactive to predictive by highlighting suspicious attributes or relationships that may be invisible to the naked eye but indicate a larger pattern of fraud.

The great value of machine learning is the sheer volume of data that computers can analyse that humans cannot, thanks to a variety of pattern recognition algorithms. With machine learning, you can add exponentially more data to your analysis — but selecting the right data and approach to model the problems is critical.

A solid machine learning-based solution also requires specialised expertise to apply rigorous methodology in data analysis and develop the fraud models to ensure consistent quality. This expertise includes carefully analysing the data, correctly treating the irregular values and data elements, dealing with bias, and validating the underlying assumption of the machine learning techniques, all whilst avoiding pitfalls such as focusing on trivial patterns in historical data and an inability to generalise the results for future events.

Traditionally, the majority of machine learning systems have strictly used supervised learning, which incorporates prior knowledge of fraud tactics to guide pattern identification, because it's easy to teach the machine once there is a clear target for it to learn.

This leads to some limitations of supervised machine learning-based fraud detection systems, including:

- Collecting and analysing enough data (historical fraud tags and transactions) to accurately identify future fraud behaviour, then deploying those models may take several weeks or months. This means it can take a long time for machine learning systems to react and prevent fraud, in which time fraudsters can do a lot of damage.
- Given rapid changes in behaviour by fraudsters to evade detection, machine learning can fail to generate an effective pattern or consistent profile, thus dramatically reducing its efficacy.
- Poor use of machine learning can generate a lot of false positives that can lead to the types of disproportionate customer challenges and friction that we have highlighted throughout this report.
- Dirty fraud tags due to mislabeling by the fraud analysts or unreliable reporting can cause the fraud model to be biased toward detecting certain behaviours that do not necessarily represent frauds.

A way to increase the accuracy of supervised machine learning-based fraud detection is to pair it with unsupervised machine learning techniques that look for irregular or uncharacteristic items, known as anomaly detection.

Anomaly detection approaches can complement supervised learning methods

Unsupervised machine learning techniques, also known as anomaly detection models, complement supervised learning by looking for aberrations in the patterns of a transaction flow. These deviations may indicate fraud, or may simply be a change in global behaviour (what "normal" looks like). For this reason, anomaly detection models generate a larger number of false positives than a good supervised learning-based model does, and are inappropriate to deploy as the only machine learning technique.

However, anomaly detection models can be a strong complement to supervised learning approaches because they approach the same problem from entirely different angles and exploit orthogonal information. When combining both techniques, the resultant analytic engine can recognise previous patterns of confirmed fraud, whilst also raising an alert if a pattern of activity changes. Making both techniques work together requires robust machine learning expertise, as the combined approach provides optimal performance – increasing fraud detection rates and reducing false positives.

Experian continues to be at the forefront of machine learning advances, developing sophisticated models that are less reliant on fraud tagging and react quickly to attacker behaviours. We view the combination of approaches as pioneering machine learning for fraud detection.

A hybrid approach: machine-based learning and characteristic-based analytics

Fraud experts are deeply immersed in studying fraud behaviour — including understanding the psychology of different types of criminals. They also have years of hands-on experience working in the fraud prevention field — and often in multiple industries. These fraud experts bring the insights needed to both guide machine learning and create characteristic-based analytics.

Here are some examples of characteristic-based analytics:

- Pinpointing new threats where not enough attack data exists for machine-learning models to adapt appropriately.
- Understanding how and where fraudsters specialise, operate, and originate.
- Interpreting behaviour that is likely to result from a fraudster's desire to cash out quickly.
- Predicting how fraudsters are likely to circumvent known triggers — such as high-value cash-outs — and known multi-factor authentication mechanisms (as discussed earlier in the report).
- Researching how vulnerabilities across the lifecycle or blended ecosystem might be exploited (such as how fraudsters circumvented mobile device security).
- Identifying the subtle difference in behaviour patterns (this is especially important as customer behaviour becomes less predictable, as not all anomalies are fraud indicators).

Emerging trends

3 advantages to the hybrid approach in modern fraud strategies

Characteristic-based (rules-based) analytics combines this highly specialised expertise with machine learning — which we call a hybrid approach to predicting fraud. There are three main reasons why Experian's hybrid approach results in better outcomes than machine learning alone:

1. **We can make discoveries faster than with machine learning alone, narrowing (or sometimes eliminating) the window that fraudsters have to do damage.**
2. **We can correlate other behaviours to make it harder for a fraudster to disappear by changing a single tactic or attribute.**
3. **We can reduce the number of false positives to develop a right-sized solution that minimises disruption to legitimate customer traffic and transactions.**

How it works

This example steps through the hybrid approach applied to a routine transaction: the purchase of an airline ticket online.

- A fraudster purchases an airline ticket using a stolen credit card.
- We use machine learning models to determine that the transaction is 20-50 times more likely to be fraudulent because:
  - The originating airport is more than 500 miles away from where the customer lives.
  - The credit card has been used to purchase three other flights in the past 48 hours with different passenger names.
  - The user completed the transaction in fewer than 3 minutes, much faster than average.
- Taken together, these variables would trigger a high number of potential frauds for review, which is likely to impact hundreds of legitimate customers.
- In order to reduce the number of false positives, we add characteristic-based learning. The fraud experts believe that the following are important factors to look at combined with the findings of machine learning:
  - Does this ticket purchase fit the customer's typical purchase profile?
  - Do the time-to-depart, class of service, and itinerary fit normal behaviours for the customer?
  - Does the purchase appear to fit any known fraudulent activities previously seen across other airlines or industries?
  - Does the device used in making the purchase have impossible device or language values, suggesting emulation fraud?

By combining machine and human intelligence, we significantly reduce the number of false positives (reducing friction on legitimate customers) and enhance predictive fraud detection (to mitigate fraud losses and brand damage).

Business Application: Tackling device emulation fraud using hybrid approach

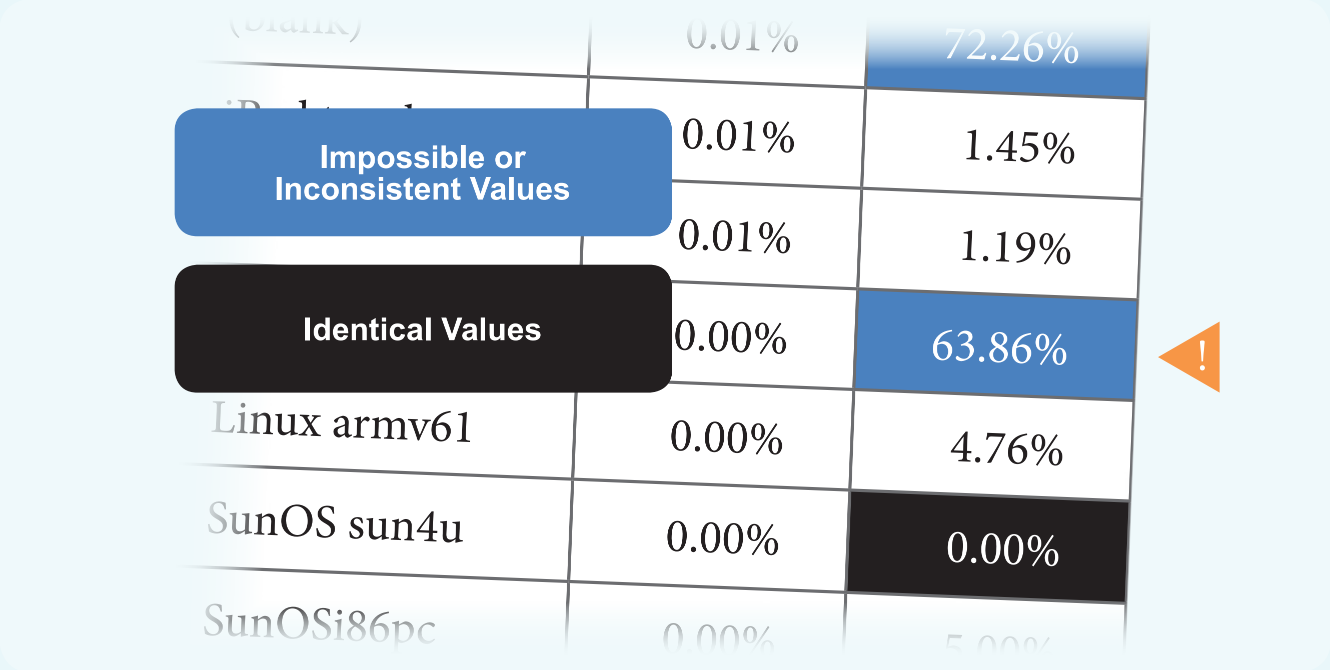
The hybrid approach has enabled Experian to achieve major breakthroughs in device emulation fraud. Device emulation fraud has been around for quite a whilst in the criminal underground. But device emulation for the fraudster masses is a relatively new phenomenon, becoming a more pervasive threat over the past 12-24 months.

How did this come about?

In order to understand the customer experience of websites and apps, Web developers leverage simple browser extensions and add-ons to run tests that emulate the characteristics of all the device types that their customers might use. As a result, device emulation software has become more widely available and easier to use — and fraudsters have taken notice.

Many companies have taken an aggressive approach to device emulation fraud by rejecting transactions initiated by devices simply having JavaScript disabled. But this approach often blocks the attempted transactions of privacy-conscious consumers, as well. Statistically, those good customers will significantly outnumber the fraudsters — which indicates that this is not a right-sized solution.

As shown in Figure 3, using a hybrid approach of machine-learning models and characteristic-based rules, Experian uncovered some careless oversights by fraudsters. Slight mistakes (like incorrectly characterised operating systems or languages) gave us the information we needed to create precise rules to catch a large population of device emulation bots. These rules successfully pinpointed impossible values or inconsistent combinations in device and browser attributes. As a result, the number of false positives we achieved was close to zero.



(blank)	0.01%	72.26%
[illegible]	0.01%	1.45%
	0.01%	1.19%
	0.00%	63.86%
Linux armv61	0.00%	4.76%
SunOS sun4u	0.00%	0.00%
SunOSi86pc	0.00%	5.00%

Impossible or Inconsistent Values
Identical Values
!

Figure 3. Machine learning-based approaches allow us to look at attack rates at the attribute-level rather than transaction level. By looking at attack rates of an individual attribute, we're able to affect decisions on transactions where those same attributes are seen. Examples of common device attributes could include platform, browser, version, language, operating system and more. The above image illustrates the number of times a particular device attribute appears (known as coverage rate) and percent of time that the particular attribute is associated with fraud attacks (known as attack rate). A low coverage rate (0.01%) means that attribute appears infrequently and a high attack rate (63.86%) means that it's been associated with or indicative of a fraudulent attempt. In this example, we saw a strong indicator of unexpected or impossible values in the platform attribute, so we manually validated and applied strategies to detect them in Experian's fraud solutions.

Fraudsters have caught onto the predictability of automated detection systems, and the inability of those system to adapt quickly to new threats. In fact, we've seen fraudsters change the pattern of their behaviours in an effort to be less predictable (e.g. shifting their User Agent String with every transaction, spoofing their IP address to mimic the legitimate user, or automating scripts to submit transactions every two hours rather than every five seconds). However with a hybrid approach, fraudsters cannot simply avoid machine-based logic. They also have to anticipate the behaviours fraud experts will target and the information sources they will leverage.

Our goal is to be invisible, so fraudsters cannot anticipate when, where, and how they might get caught. And we want to minimise disruption to legitimate customers, so they feel protected without being inconvenienced or, worse, mistreated.

Conclusion

Criminals have created a business from committing fraud — a source of success, reputation, prosperity and innovation. For companies, preventing fraud loss is often viewed as a cost of doing business, and, as such, is approached defensively. In order to outpace fraudsters, organisations are modernising their fraud mitigation strategies, making them less reactive, and more predictive and proactive. To that end, fraud teams are becoming an integral part of creating sustainable business growth by adopting several principles including these:

- Creating an ideal customer experience as a shared goal of fraud, product development, and marketing teams (these teams no longer work in a siloed fashion).
- Sharing information across functions (fraud teams, marketing teams, product teams, among others) to gain an expansive view of customer behaviour.
- Collaborating across the customer touch points to facilitate pre-transaction fraud detection, thereby reducing capital and operational expenditures.
- Using a blended ecosystem (working with vendors, customers, partners and even competitors) to increase agility.
- Applying the appropriate degree of confidence, based on the nature of the transaction, to optimise resources and streamline the customer experience.

Weaving these principles into your fraud strategies is crucial for success, because fraudsters are relentlessly fast — and getting faster. One of a fraudster's biggest advantages is the ability to move through a consumer's online and offline life without boundaries — swiftly preparing, attacking and moving to the next vulnerable area where you build relationships with your customers, across channels and at different touchpoints. With advances in fraud detection analytics and technology, ecosystem participants like Experian can help you confidently recognise your customer and protect your valuable relationships.

Modern fraud mitigation approaches have shifted fraud prevention from "the cost of doing business" to an important driver on the growth agenda, with an active role in a company's success. Because we understand this dynamic, we can help businesses effectively fight fraud whilst providing a first-rate experience that inspires customer loyalty — and results in achieving ambitious growth goals.

> **If your competition does a better job than you of modernising fraud detection, then fraudsters are likely to view you as an easy target. Being status quo does not afford protection these days — it is another form of vulnerability**

Experian CrossCore™ future-proofs your investment choices

Experian's CrossCore platform is one of the most significant advances in the modernisation of fraud prevention. CrossCore is the industry's first smart, plug-and-play, open (API-based) platform for choosing and changing tools, services, and information sources. You can confidently keep pace with your company's products and services, customer needs, regulatory requirements, and the latest in fraud tactics.

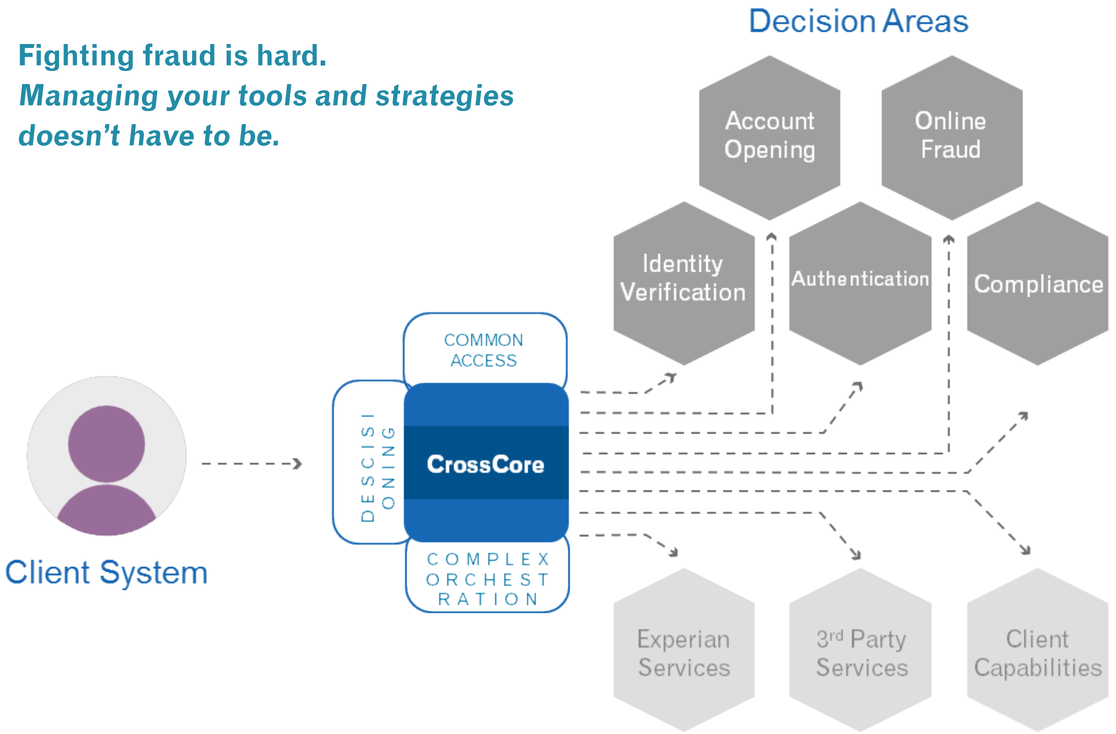
Be as nimble as fraudsters in using the best technology available. You are essentially future-proofing your investments, because updating and changing can be done with the flip of a switch versus a lengthy implementation. No more worrying about falling behind the technology curve.

CrossCore is offered as software-as-a-service (SaaS), so there is no capital expenditure associated with purchasing, deploying or updating any technology.

Because CrossCore is an open platform, you have the advantage of an expanding universe of solutions — your own, Experian services, or third-party tools. You can link your own internal systems through CrossCore to manage services through a single access point and create sophisticated, multi-layered fraud prevention without the associated complexity.

Catch fraud faster, improve compliance and enhance the customer experience. To find out more about CrossCore, visit www.experian.com/crosscore

Fighting fraud is hard.
Managing your tools and strategies doesn't have to be.



Explore More

Corporate headquarters

Experian plc
Newenham House
Northern Cross
Malahide Road
Dublin 17
D17 AY61
Ireland
T +353 (0) 1 846 9100
F +353 (0) 1 846 9150

Corporate office

Experian
Cardinal Place
80 Victoria Street
London
SW1E 5JL
United Kingdom
T +44 (0) 20 304 24200
F +44 (0) 20 304 24250

Operational headquarters

Experian
The Sir John Peace Building Experian Way
NG2 Business Park Nottingham
NG80 1ZZ
United Kingdom
T +44 (0) 115 941 0888
F +44 (0) 115 828 6341

Experian
475 Anton Boulevard Costa Mesa
CA 92626
United States
T +1 714 830 7000
F +1 714 830 2449

Serasa Experian
Alameda dos
Quinimuras, 187
CEP 04068-900
Planalto Paulista
São Paulo
Brazil
T +55 11 3373 7272
F +55 11 2847 9198

Contact us here, or email: eda@experian.com

Local Insights from Experian’s Thought-leaders

Fraud Prevention Benchmark Tool | Global

The Economics of Fraud 2016| Asia-Pacific

Fraud Report 2015 | India

Interactive Fraud Analysis Tool | United Kingdom

Fraud Attack Heat Map 2015 | United States

Digital Marketer Benchmark Report 2016 | United States

Decisioning 2020 | Europe, Middle East, Africa

Data Management Benchmark Report 2016 | Global

Experian