DEVICE FRAUD DECTECTION

FRICTION-RIGHT CUSTOMER ONBOARDING

REPORT

TransUnion

PassFort

FIGHT FRAUD & CREATE FRICTION-RIGHT CUSTOMER ONBOARDING

INTRODUCTION

Gavin Barker is channel manger at TransUnion, formerly iovation, and has worked in the ID and Anti-Fraud space for 20+ years. Five of those years have been in digital fin crime, looking at the use of technology such as smartphones and other devices, and educating businesses globally on how to enhance their risk strategies based on these technologies.

Gavin has experience in various types of risk mitigation tools and has worked with TransUnion in Financial Services on an international scale.

Here Gavin and PassFort's Head of RevOps, Tom Andrews, talk about the spikes in fraud and risky behaviour in recent months, the quick and simple way device fraud detection can combat financial crime and how this dovetails into friction-right customer lifecycle processes like onboarding.

ACKNOWLEDGEMENTS

Thanks to Gavin and TransUnion for their time and contribution to this process.

UPS AND DOWNS CREATED BY THE COVID STORM

Tom Andrews: What's the current backdrop for risk and fraudulent behaviour - how does TransUnion see that right now?

Gavin Barker: COVID has changed a number of things and there have been winners and losers. In some verticals the impact has been negligible - some businesses are even excelling.

In Financial Services, a lot of the origination and the application style volumes have dropped away. Many lenders simply have not been lending during this time, so that's had an impact.

However, what we've seen is more interactions at places like login – these have increased because people are more conscious of looking into their bank accounts at the money they have available.

In other sectors we've seen significant drops in activity, hotels and bookings industries for example, and airlines too are massively down of course.

But when you look at e-commerce, TransUnion's transactional volumes across e-commerce has been above 20% compared to the same period last year.

When you split that 20% into certain sectors of eCommerce, there have been huge winners. Gaming, not online gambling but specifically gaming, has seen more than 75% increase in TransUnion transactional volumes because people and families are at home, so they're purchasing games and downloading them onto their devices.

"Companies with fully digitised journeys are definitely prospering better."

From a fraud perspective we've seen an increase in what we class as “risky device” transactions. This means more interactions ticking red flags and triggering rules for our clients. We've seen an increased amount of evidence placement in this period compared to the same time last year, because things that are high risk have been identified and there's more fraud happening.

Specifically, on fraud, we're aware there's been a spike in the number of phishing attacks and scamming activities. A lot of phishing attacks are very professional, and people are falling for them no matter how much education there is.

I had a phishing scam myself, [someone purporting to be] from the DVLA. It did look very genuine. Luckily, given my background, I'm skeptical when people reach out to me with these kinds of things, but there has been a big increase in this area.

"TransUnion did a poll recently and more than 29% of people poled had a phishing attack or some kind of social engineering attempt in the last 3 months."

Riskly transactions are being fuelled, because a lot of time [fraudsters] are carrying out activities, but they're not necessarily getting someone to pay for something there and then. They're looking to harvest personal information such as email addresses and attempting to get login credentials. They use this data to further perpetrate fraud, creating synthetic IDs, attempting account take overs. Risk and fraud direct to consumers and to business customers has certainly spiked.

Tom: Talking about patterns of behaviour - one thing is people working from home, using personal laptops instead of a work laptop. We're also seeing companies that historically perhaps sold gin are now creating hand sanitizer. In terms of change in behaviour or business, how does that impact the risk landscape?

Gavin: From TransUnion's perspective, we're very much device centric. Looking at the device aspect of this, typically we operate in a business to consumer channel or business to business in a commercial lending scenario. What we've seen and where we're helping customers is with staff working from home and using different devices to connect to internal and external websites to carry out work, which brings potential risk to those businesses.

"We're having more and more conversations about enterprise authentication or enterprise security."

We are looking at the devices staff use to connect to sites and making sure they're only accessing what they should and that the devices they're using are not risky in some context. We want to make sure they're not susceptible to malware for instance.

There has been a change in some of the conversations we're having from the standard business to consumer side. A number of companies have been "adopting and building out" their digital channel for a while now, and because of COVID those companies that might not have had a fully digital immersive channel for consumers have made it their number one priority.

"Businesses are looking to change their processes and asking: How do we onboard customers in a fully digital way?"

How do we allow customers to log into accounts to do the things they want and make purchases, or transfer things without having to do some manual intervention?

There has been a huge ramp-up of customers across verticals looking at getting their digital channels unlocked. That's the way the world is going and it's never going to go back.

A lot more companies are enhancing digital journeys. With that comes questions about mapping out risk mitigation.

- What do we need in terms of risk mitigation?
- What risks are we going to be exposed to?
- How do we effectively layer services, so we're protected?

Tom: Before going deeper into the digital customer journey, can you give us an overview of how device fraud detection works?

Gavin: TransUnion offers device risk intelligence. Essentially, we're looking at the devices used by your customers when they're interacting with your digital architecture. When people onboard customers, there are a number of checks they do. Some are for regulatory reasons, some are good practice. ID validation, for instance, PEPs and sanctions are all regulatory requirements.

What we've learnt over the last 25 years of people becoming more digital is when you go online (if you have an app or use a website) you open yourself up to more risk because the transaction can come from anywhere at any time.

TransUnion, formerly iovation, is driven with the purpose of making the internet a safer place to do business.

We looked at the common denominator across all digital channels and all interactions and that was somebody using a device to interact.

"We asked - can we extract data from these devices that would allow businesses to make more informed risk decisions."

TransUnion can profile a device - sometimes it's referred to as a fingerprinting. Using JavaScript and SDKs so when your consumer is interacting with an applications page for a financial services company and they're going through their normal processes of filling in their data, our JavaScript will essentially profile the device being used.

We don't capture personal data; we look purely at the device. We're looking at things like: has TransUnion seen this device before within this network? We recognise the device through our network and can collect upwards of a hundred different attributes, including:

- Operating systems
- Browser languages
- Screen resolutions

All this data can be taken by end users to build risk rules. Certain characteristics might indicate high risk, like geolocation for instance - where is the device actually coming from? If an applicant is telling you they come from Leeds, in Northern England, but we backtrack that and find it's from somewhere else, our end user can decide if it's a potential risk.

Then we have a global network consortium, which is very powerful.

"TransUnion has more than 83 million fraud records uniquely assigned to devices in our network."

If a device has got a reputation or a history of fraud, and that could be things like application fraud, payment, fraud, synthetic ID, we can get very granular on these different types and share the data with our customers.

The scenario would be you stop a returning 'bad device' from coming back to your business, and if the device has been seen by other customers [in our network], when it comes to you for the first time, you'll instantly get a flag to tell you that device has got history.

Essentially, we're looking at the devices being used and extracting data from them, then we use additional data insights to allow businesses to make informed risk-based decisions about potential threats.

What we've also seen in recent years is a big push around monitoring at login. We have the capability to sit at the login touchpoint. We can tell you if a device attempting to access an account is a device that should be accessing it.

In a nutshell, leveraging devices that are being used when they interact with a digital infrastructure, pulling data from them that wouldn't otherwise be available and allowing companies to use that data to make thorough, informed decisions.

"Firms can spot different patterns and transactions that would be missed with traditional ID proofing technology."

The fact that it is device-centric is powerful because a lot of times when you look at things like synthetic ID, the personal data is compromised. If you make an assessment purely based on that there is a risk you will validate the ID exists, but you also want to be able to validate that you're interacting with the owner of that identity.

"The tricky element is validation in a digital world so it doesn't put friction on a customer."

If you introduce friction, consumers jump. Device risk intelligence runs invisible to the consumer, it’s in the background. You're not impacting the customer journey, but still pulling insights that otherwise would have been missed.

It's a very complimentary service with a lot of other kinds of onboarding processes. It's an additional tool in the risk mitigation process.

Tom: Do you see device fraud intelligence adding together with KYC and onboarding to create a new digital customer experience that consumers need and that protects them against risk in the online world?

Gavin: I've seen more and more companies adopting device-risk services in different guises, whether they've formulated something internally or leveraged services like TransUnion.

Adoption has increased as companies realise their risk exposure. It's become more apparent that device-fraud detection is no longer nice to have it's a need to have. It's an additional layer in risk adoption.

If you've got a weakness in a certain service, for instance, if you're relying heavily on personal data and that personal data is compromised, then layer it with something that's going to fill the gap and device-fraud detection does a fundamental and powerful job there. It doesn't degrade the customer experience, which is so important in a digital channel.

"The future is going to be that most companies will be leveraging device intelligence. They may bind it with other data they have to formulate a digital persona."

Tom: Something I've noticed is an increase in the prevalence of two-factor authentication. I can rarely login without my mobile in hand. Do you think the increase of solutions like device-based fraud detection is even more important because someone could spoof my phone or steal my phone and suddenly log in to everything?

Gavin: Two-factor authentication has been adopted widely through a number of different verticals, including financial services. We've seen it in insurance, telcos and a number of other sectors. Potential risks come with it, depending on what you're using within that two-factor setup.

If it's a phone number and you're sending an SMS, the user experience can be degraded as well as their being potential risks that you get from things like SIM swap. Two-factor is good and more companies will start to use it, but look at what mechanisms they use within that.

The device, to me, seems very powerful because most people are going to have a device in their hand. Rather than having a process that you have to do an outbound 'come to me to get me to authenticate, instead looking at things like device-based authentication, where you compare the consumer's device specifically to their account so when they log in you can validate the device is the right one for the account instantly.

"It gives a much better user experience and it's done in a more seamless and friendly manner."

I think we'll also see adoption of multifactor authentication, where you leverage the device but allow the consumer to pick from a number of different ways they want to passively authorise and authenticate themselves.

Things like using SMS and OTPs will start falling by the wayside. There's going to be other ways to do outbound comms. In our technology, we use real-time push notifications for instance.

Tom: What success metrics do you have for firms using device fraud detection?

Gavin: It's the million-dollar question and it's something we're keenly aware of. Whether we are entering into a POC [proof of concept] with a company or even a live deal, one thing we're keen on is understanding our customers. What their fraud challenges are and everything else starts from there. We need to understand what the problem is we're trying to solve, and the size and scale of the issue. We ask and find out and work with customers to understand how many fraud events they have per month. The average cost of fraud. Then we can start to build tangible actionable metrics off the back of it to define what success looks like.

"Typically when we're looking at the financial services world, a key metric is an X percent reduction in the cost of fraud or an X percent increase in the identification of fraud and risk."

We've worked with a number of companies and have a number of case studies that are publicly available where we've returned high value ROI.

One of our customers for finance that uses us globally saw 40% reduction in fraud through their origination journeys. Only when they started using the device detection were they able to suddenly get visibility into data that they hadn't seen before. They could identify quickly and simply things like a device applying for a hundred different loans in a 40-day period using a hundred different peoples' personal details. As soon as you put the device aspect into it, it's almost like a blindfold-off moment. They could see it was hugely risky and not normal behavior.

Key metrics typically look at things like reduction of fraud and increase in detection. When we talk authentication, it's more of a challenge because when we're protecting the log-on it might be that a key metric is looking at the reduction or detection capabilities of an account takeover attack or a brute force attack - and they're quite tangible.

ROI based on financial impact is different, because there's the financial issue of a possible breach and a fine that comes further down the line. There's not a quantifiable number up front to build a metric from. So metrics vary a little depending on the touch point, but the key ones are increases and decreases in fraud detection.

Tom: We've talked about digital customer experience, are you seeing a variety of clients starting to look at that as part of their success metrics - speeding up that process or making it a more usable one for the end consumer?

Gavin: Definitely, as companies have started to look at their digital channels and various stages of their digital journey. They will also continually look at how to enhance it; how to make it better?

Some of the metrics around this are quick and simply - how do we make the time from the consumer applying for an account to being accepted quicker, without increasing exposure to risk or falling foul of regulation or the law?

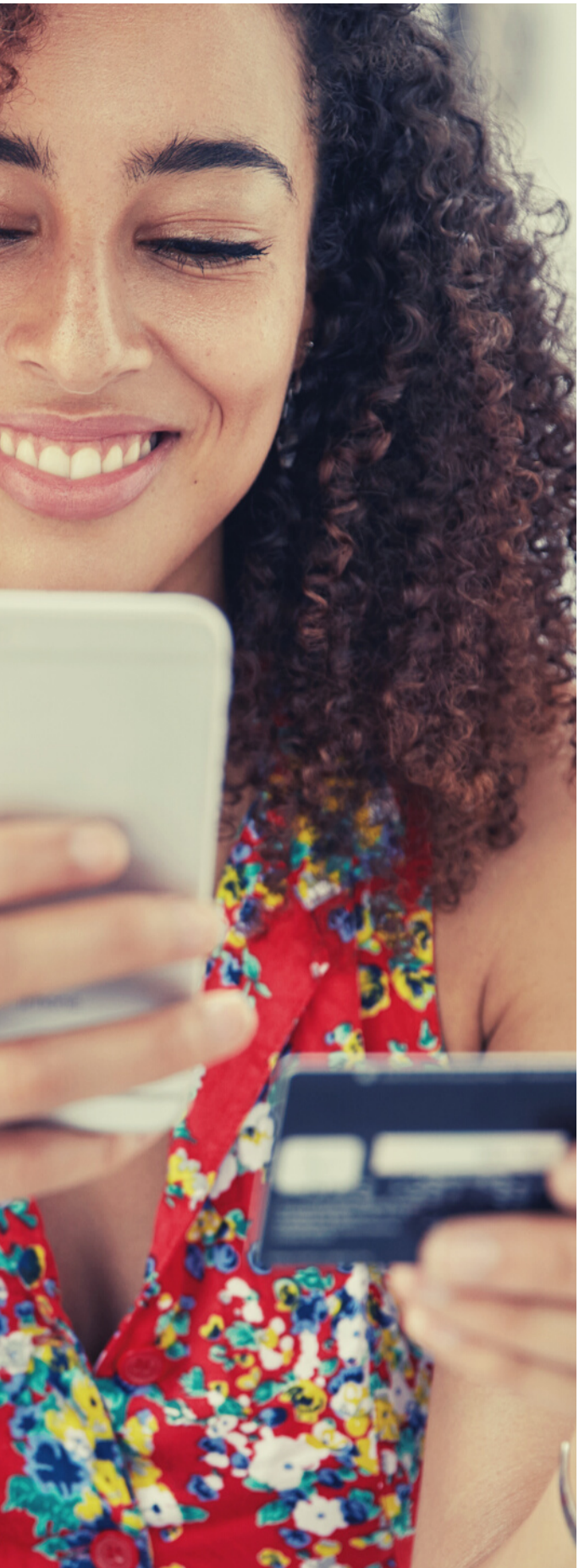
"Customer journeys are a big thing for companies. It's not just about real-time risk mitigation and fraud detection. Obviously, they are incredibly valid, but more and more user experience teams are involved in conversations because whatever you introduce could have an impact on the consumer flow, so they want to make sure it's a good flow."

Nobody wants to put barriers up in front of a customer because consumers are fickle. The user experience is hugely powerful. It's got to help and enhance your risk services and help you fight fraud in the channel, but it can't come at the cost of user experience because if you have a bad experience, you're going to lose customers. You'll see basket abandonment and dropouts - it's never going to be good for your business and you're just going to drive people to competitors if they've got a better experience.

Tom: Final question, what are your thoughts for the future?

Gavin: From a device perspective, we're halfway through the realisation of companies that device risk intelligence is essential. Now we see more customers engaging and more RFIs where device is specifically called out. Companies are seeing the value of it.

I think that is going to continue as the world moves digital across every vertical. Consumers don't want to go in branches or in store to do things when they can download an app and have it done in seconds.



BEST PRACTICE IN CUSTOMER LIFECYCLE MANAGEMENT

BEST PRACTICE SERIES

Knowledge of device risk is expanding. It is becoming a formal part of onboarding journeys. The challenges of synthetic ID aren't going away, neither are ID breaches. But as fraud evolves, firms are adding layers to their processes and device is a fundamental one.

This episode in our best practice series has been about finding out how to combine compliance checks, so if a device ID has been involved in fraud and tries to apply for a product, firms know they are a potential risk before further validation is needed.

For more information email **info@passfort.com**

ABOUT PASSFORT

PassFort offers a single SaaS solution for full customer lifecycle management. Headquartered in London, PassFort serves financial institutions of all types and sizes, processing more than 150,000 compliance journeys each month.

www.passfort.com | info@passfort.com

ABOUT TRANSUNION

TransUnion, formerly iovation makes it safer for to do business online. Instantly knowing which devices can be trusted and which can't.

www.iovation.com