Payments on Fire®

Episode 140 – Finding Fraudsters at the Front Door - Robert Capps, NuData Security

George Peabody:

Welcome to Payments on Fire, a podcast from Glenbrook Partners about the payments industry, how it works and trends in its evolution. I'm George Peabody partner at Glenbrook and host at Payments on Fire. Payments on Fire listeners know that we've been taking a steady look at fraud issues. Fraudsters have been pouncing on every opportunity taking advantage of the pandemic relief payments, as well as the shift from a card to card not present, what we call remote commerce transactions.

And God knows the pandemic has been a forcing function in that area, and measuring what the fraudsters are up to and their impact is really critical. To talk about some of those key metrics, I'm delighted to welcome to Payments on Fire, Robert Capps. He is vice-president market innovation at NuData Security, a company that specializes in behavioral biometrics. Robert, really glad you're here.

Robert Capps:

Thanks for having me.

George Peabody:

Robert's firm NuData published during the Summer off 2020, its first half Fraud Risk at a Glance report on cybersecurity trends. And the findings are really interesting. But Robert, before we get there I want to ask you to indulge me to understand, first of all, how you found out what's going on? And that's going to require some discussion of fraud management in general and then your role in it.

Let me just start with the fact that fraud management, particularly across financial institutions and merchants, but because merchants own the liability it's a multi-layer discipline.

You've got to have multiple tools, multiple providers in a number of these areas to be able to successfully remediate fraud, keep it in its box at the right level. And that there are multiple techniques here, this post attack analytics to identify transactions that have resulted in fraud, there providers who on the other hand offer guarantees for an individual transaction. They'll cover the charge back. And there's a stack of tools in place to detect and prevent fraud. That's where NuData comes in. So let's talk about that stack in general terms, how would you describe it? What's the set of tools in typical use today?

Robert Capps:

Yeah. So the tools, they actually vary based on the industry and based upon where you sit within the industry. There are some organizations that simply deal with a lot of guest transactions, predominantly guest transactions. And the mixture of tools you put in front of those transactions is often going to be different than those where you have a regular interaction with consumers and get a good bead for their interactional profiles, their devices in use, their behaviors and things like that. So in general, though, everybody has liability somewhere, right? It isn't just card not present and liability shifted to the merchant.

Robert Capps:

If you think financial institutions, they very much have liability in that transactions that originate on their online banking platforms can result in large dollar losses to the institution when they make the consumers whole. You also have the issue of customers not feeling safe at an institution once something like that's happened. So if someone comes in and transfers $10,000 out of their account, they might be reluctant to do business with that bank gain.

George Peabody:

I have no idea why. I mean, golly.

Robert Capps:

Yeah. I mean, in a lot of cases though there's no clear at fault for these sort of situations other than the fraudster themselves. So we're definitely not calling out a financial institution as being deficient in their protections or anything. Some of these situations originate with a consumer using the same username and password on many sites, including their bank. And so it's not hard to get ahold of good consumer accounts these days with account takeover fraud continuing to be a major contributor. You need to have technologies in place that can identify when the right consumer's in place and the right consumer is actually interacting. So yeah.

George Peabody:

So what are those technologies?

Robert Capps:

So from our most organizations, you're going to need something around new account opening and account login. Those are the two primary mechanisms where the bad guys get in. And so around new account opening, understanding whether the account is originating from a human or from a bot, a script, malicious software, is a big deal. So bot detection and mitigation is important at that point. Once you've screened off the technology, right, the technological attacks, getting down to is this human behaving like a normal human would. So behavioral analytics using understanding how this consumer is interacting with the page flow, but say an application, is it normal the way they're behaving?

Robert Capps:

Are the speeds normal? Are they going through the correct number of pages when they're entering data into those pages? Do you see that they're entering them in order? Or are they sort of popping around the page putting data in, or is it just appearing in a page, right? So they're using a form filler or some sort. And so these are sort of behavioral elements that can be utilized to identify risks within the interaction. And then when you get past the interactional risk, taking the data itself and running it through data validation tools, are there sort of public and privately available databases to verify that these data elements belong together, data consortiums that are available, different organizations security products have these data consortiums that you can use to verify legitimacy of data.

Robert Capps:

So there's a lot of steps along the way of new account fraud, different technology stacks, different providers that can be used to augment your new account risk strategy. When we go to account takeover, we get a log in, protecting login. Some of the same automated tools are germane to the transaction, right? So is this logging occurring because a human loaded a page and it's typing things into a form, or is this logging occurring because data was just posted to the log-in API.

There was no page loaded, no JavaScript executed, no form filling identified. And so, that same sort of automated detection of human versus non-human behavior, very important. Understanding the velocity, understanding the way that data is being input into the page in human interactions, very important. Device technology, looking at device connection location, device intelligence, still a very appropriate technology layered into the stack[crosstalk 00:06:39].

George Peabody:

So you're talking about IPG location and that kind of thing, or looking at it the software profile on the device?

Robert Capps:

Yeah. Device ID. Yeah. I mean, it can be as simple as a simplistic device ID and looking at the history of an IP. It can be as deep as getting into fine-grained location services as provided by the device itself. And there's lots of variation in between those things. And then getting into understanding credential compromise. So we know that when data breach happen username and passwords are compromised, there's a period of time where those data points are used privately by the attackers or the groups that stole the data.

Robert Capps:

And then over time, more and more of the data gets sold to other fraudsters who are able to leverage it. And so as those sales happen, there's an opportunity to start to see valid username and password combinations that can be identified as far as overlap with existing customers at an institution or an e-commerce provider, or what have you,

George Peabody:

In other words, you've got the afternoon to go out and out of the dark web, buy those credentials yourself, and then compare them against your own.

Robert Capps:

Obtain, sometimes you buy, sometimes you don't. But is it stealing if you're taking them from a fraudster? No, I'm kidding. There are commercial services. I mean, they're commercial services that an institution or an e-commerce provider can subscribe to, to get data as it is compromised so that they can proactively immunize the customer base. If they know they have a customer that has a compromised credential, it's only a matter of time before someone figures out that there's overlap and tries to attack that account. And so, the more proactive an organization can be to identifying those accounts, better off they're going to be.

George Peabody:

Where does what NuData does fit into this overall stack, and what are the functions that are adjacent to you? How do you fit into this set of tools that help a bank or a merchant detect and manage the fraud?

Robert Capps:

The best way that we fit into that solution is we provide a blended set of solutions are integrated together and leverage one another. And so, a lot of what I just talked about in regards to e-commerce and financial services fraud which originates at new account and login, a lot of that is covered within the solutions we provide to our customers. And so, a great example of that would be we do fine-grained automation detection. Looking at not only the brute force, very

unsophisticated ATR, automated transactions but also those that are human emulating. And so, if you look at financial institutions about 96% of the attacks we're seeing now against financials are this human emulating attack where pages are loaded, JavaScript is loaded, graphics are loaded, forms appear to be filled out like a human would normally fill them out.

Robert Capps:

And they're done in order and velocities that look like human. And so, that fine-grained as well as the core screened automation that's something we detect and we can help remediate at the front door. We do passive biometric verification. So we're looking at things like typing speed. We're looking at things like the dwell time between key clicks, when you type your username. The dwell time that you hold a key down, the confidence in which you type those things. You're not hunting and pecking and stopping and starting.

George Peabody:

Are you building profiles then of that behavior that are then attached to individuals?

Robert Capps:

Yeah. So understanding whether or not automations present, understanding the device, the connection location, the device intelligence, understanding the passive biometrics and as well, the behaviors of all of those elements, we're able to build anonymized profiles that allow us to identify whether this human is interacting with this account over a period of time and to identify when things diverge from that profile. Yeah. And so, that's really key to understanding account takeover. Whether you have my credentials or I have my credentials only, I should be able to log in with those, even if we both both hold valid credentials, the system's gotta be able to differentiate between you as a human and me as a human on any given account. And that's the magic of what a NuData brings to the market around those areas.

George Peabody:

Do you generate a risk score?

Robert Capps:

Yeah. So we provide confidence factor, how confident we are this is the same human. And then based upon different signals that are observed within the interaction, we can provide a relative risk score and even color banded responses, red, yellow, green, reject review, accept. Yeah.

George Peabody:

So will you be the entire fraud stack for an e-commerce merchant, for example, or do you fit into a stack where you'll hand off the score and the merchants can use some other tools, whether it's a rules engine or something else looking at the transaction and bringing together before they send off for authorization?

Robert Capps:

That's really up to the customer, to be honest. We can handle new account, we can handle login as a contained use case and be able to provide back a high confidence score and decisioning for that you use case. When it comes to things like transactions, wires, money movements, e-commerce checkouts, things like that we tend to layer our intelligence as an input into risk engines and other decision engines that the customers will probably already have. So what we do at the front door

can be standalone. What we do at the front door can be blended with other tools, depending on the strategy of the organization that's adopting our technology.

Robert Capps:

Often in most cases, what happened at the front door is carried on through that session to understand whether the ultimate transactions that occur are trustworthy. And so, knowing that there's a low probability match at login means maybe you want to step up a resulting transaction in that session through some other mechanism. But for low risk interactions, like looking at a balance or, looking up other non-critical information, you might not really put friction in front of the customer. And so, it puts the control of friction and impact on the customer experience in the hands of the organization that needs to balance the friction versus the safety of the transaction.

George Peabody:

You talked about your role in following the transaction as such a versus the very front door up to the checkout page for example, that suggests to me that there's an implementation process where your code has to be invoked throughout that journey from the very front door, at a website to the checkout page. How's your solution implemented then?

Robert Capps:

It's implemented in really in two parts. The first part is JavaScript that gets integrated into a webpage and some additional fields that are placed on those pages to collect information from the JavaScript, that information is submitted back to the organization as deploying our solution, and they gather that data and some additional data around the service side of the transaction. And that data is submitted back through an SDK we provide our clients back to our service for scoring.

Robert Capps:

And so, the roundtrip occurs between the consumer and the organizations using our product, and then between that organization and ourselves. We never get in between the customer and the institution or the merchant. That gives them the ability to control what data is transferred. It also gives them the ability to do final sanitisation of data before it's sent back to our solutions so they're not sending us wrong credit card numbers or socials or things like that. And so we very much-

George Peabody:

They don't want it either, if there's so-

Robert Capps:

Yeah. I mean, and we do work with, when we talk about payment types and payment, we do have the ability to work within some of the tokenization strategies that the innovations might be using at the merchant level and NuData also provides a product called Smart Interface which is our EMV 2.0 3DS solution. Did I get that in the right order?

George Peabody:

Yeah. I think you did. Yeah

Robert Capps:

Anyway, so many acronyms.

George Peabody:

That's right. NuData, you should be clear is a MasterCard company so you've got integrations into the sort of MasterCard gateway service.

Robert Capps:

Yeah. Well, and we're also a part of the connected intelligence strategy for MasterCard, which brings together a lot of the adjacent businesses they've been acquiring over the years from RiskRecon, Ethoca to Brighterion and NuData and so on and so forth. A lot of that technology is integrated and being integrated so that information we pick up at the front door during a transaction will eventually be available to merchants and issuers through Ethoca and some of their solutions. So in other words-

George Peabody:

In other words you've got the whole stack.

Robert Capps:

Yeah. I mean, we really look at it from external scanning for vulnerabilities and potential compromise with the RiskRecon acquisition to the consumer verification pieces around consumer identity and new account openings with NuData. And you look at Brighterion with the machine learning and the large data analytics, and then Ethoca dealing with chargebacks and electronic receipts and things like that. You can start to see that strategy of why MasterCard was acquiring the companies they were over the last few years.

George Peabody:

Thanks for that picture of where you fit and what you've done and the role that NuData's got. Now let's turn to your report, which is what peaked my curiosity in the first place. So this report you published this Summer looking at the fraud trends for the first half of 2020, what are some of the high level findings, what'd you find out?

Robert Capps:

Commerce was up ended.

George Peabody:

Oh.

Robert Capps:

COVID had a really large impact with the lockdowns and things, really had a large impact on the movement of transactions from physical world to virtual commerce transactions.

George Peabody:

So you saw a lot more activity than you had before?

Robert Capps:

Yeah. I mean, the benefit of being a MasterCard company is, we can also look at other types of transactions. And MasterCard doesn't only look at MasterCard transactions or credit card transactions, there's VocaLink and there's other organizations that MasterCard owns that have other modalities of transactions. So a lot of what we see is not necessarily credit card transactions,

but also ACH and direct debit and whatever type of transactions flowing across our different duties and [inaudible 00:17:37].

George Peabody:

And that's because NuData is not only employed by e-commerce merchants, but also you've got a role in financial institutions.

Robert Capps:

And health insurance and social networks. And so, I don't think that people appreciate necessarily the breadth of organizations that we protect. And it isn't just financial. It isn't just retail, but there are other organizations who have customer log ins that protect data behind the scenes that they want to keep to only their customers. And so, there are a lot of organizations that have deployed our strong login protection technologies, and a new account detection technologies in order to protect their customer base and their organizations. And it's not just about wire transfers and e-commerce checkouts, there's a lot more to what can be protected with technologies like this.

George Peabody:

So I assume then that a lot of what you found is that account takeover continues to be a really big concern, and it's probably even more serious than it was before.

Robert Capps:

Yeah. I mean, we just keep seeing data breach after data breach and the testing and understanding at this point is that there are so many breaches we just don't know about yet. And we're seeing that data becoming available on the dark web and fraudsters are using more and more targeted data against institutions in order to attack accounts. And so, when we look at things like ATO, there's a massive attack on the financial industry. We're now starting to see that even moving into streaming media, you think about people being at home, they want access to television shows.

Robert Capps:

They want access to other things to keep them occupied while they're stuck inside their homes. And so, streaming organizations that are streaming television shows, movies, audio, music, they're starting to see account takeover attacks against their accounts as well, just to get access to media and so-

George Peabody:

Wait a minute. So the motivation of the hacker is to just take over an account so they can watch Game of Thrones?

Robert Capps:

Or they can sell access. Yeah. They can sell access, one time cost of the username and password. And for a lot of organizations, they haven't necessarily been as focused on inappropriate access to existing accounts because there's no attempt to steal funds, there's no attempt to steal goods or anything like that. They're just sort of parasitic use. But when you start looking at licensing costs for media, you start looking at streaming costs for media, there's a definite tangible cost to allowing a parasitic use of those accounts.

Robert Capps:

And so, I think that you're starting to see more and more organizations focusing in on how to protect against those inappropriate account usage. And so, we were seeing a lot more pickup of our technologies now protecting streaming media because they want to make sure that only legitimate users are accessing those accounts.

George Peabody:

Fascinating.

Robert Capps:

Yeah.

George Peabody:

So let's switch over to financial institutions. What are you finding that they're most concerned about? Is it account takeover because that's where the money is or are there other particular-

Robert Capps:

That's a big piece. But you got to move the money. And so, we're seeing institutions being very concerned about mule activity, money mule activity. So once you wire money, you have to wire to another account. Most institutions have controls in place around international wire transfers and international direct debits.

Robert Capps:

And so, you have to move the money to another account, so it can then be withdrawn and then transmitted internationally in another way. Whether that's through putting cash in envelopes and mailing it or using wire transfer services or are sending gift cards through the mail, whatever it happens to be. So understanding how to protect against those mule accounts is really important.

George Peabody:

So walk me through how you get involved with that.

Robert Capps:

Yeah. So looking at, again, the new account opening process, making sure that accounts are being opened in mass to create mule accounts. So using either synthetic identities or real build name fraud, real consumer identities to create accounts online. That's really important to institutions, making sure that automation isn't being used, that human farming isn't used. I don't know if you're familiar with that term, but essentially we're now seeing evidence in all industries, actually, of organizations who are committing fraud hiring people, humans in call center environments around the world in order to fill out forms, to checkout on e-commerce sites, to do other sort of manual human transactions so that they can get around automation detection and a lot of these basic rudimentary fraud technologies that a lot of organizations have rolled out over the last couple of years.

Robert Capps:

And so it gets really interesting. The rabbit hole gets really deep, that's for sure. And one of the things we're seeing now is actually a blending of humans and technology. We have a financial services customer who is seeing about 100,000 transactions a day against their login page. And we were assisting them with looking at their automated transactions and we were identifying

automated interactions about 100,000 a day at that this profile that we would serve a capture to, and that capture was being solved at nearly 100% success rate. And so, most organizations would step back and go, huh, okay. Detective's automation, solved a really hard capture, 100% rate, maybe this really isn't automation. But because we are a blended solution looking at not just the fact that capture was served because of automation that was solved.

Robert Capps:

We're also looking at when it was solved, where it was solved and how it was solved. We could actually discern between the two transactions of the login and the capture, and we could actually identify the capture was being solved on a different computer, in a different part of the world, it had a different language in the browser and a different times zone setting in the browser than what the original transaction was, purporting to be. And so, that discrepancy law allowed us to identify that there was actually a human farm element that was handling all of the captions and all of the challenges that the automation was experiencing.

George Peabody:

And the ones that got through, then I assume that the organized hackers would pass those credentials that worked to someone who would actually be able to initiate them moving the money.

Robert Capps:

Yeah. Yeah. And because we had this consolidated view of those different elements, we could coordinate and we could measure in each of those layers, we could identify those splinted attacks in a normal sort of a set of a la carte solutions that a lot of organizations would place. They would buy a bot detection from their cloud CDN provider or they might buy it for their data center because it's available in their content distribution network internally, their load balancers or whatever.

Robert Capps:

Those technologies will block the automation but if the automation is able solve a capture, they assume it's okay and it sails right through because we were looking at each of those elements and together we could see that there was a problem, even though these captures were being solved there were still a problem with the transaction. We're able to shield the institution against almost 100%. No one wants to say 100%, so I'll say 99.9%.

George Peabody:

Never ever.

Robert Capps:

Never say 100, right?

George Peabody:

Well, even if you do, that only last for a certain period of time given the elevation of the hackers and the tools they've got.

Robert Capps:

Well, and they change it. Yeah, they constantly change techniques, but this technique stopped after a very short period of time because it wasn't successful. Now, we've heard of the similar technique being used at other organizations and they end up calling us because the word's gotten out that we figured out how to deal with these things. But you're right, I mean, I've been in this industry for way more years than may want to admit at this point. And I've seen some very technically beautiful attacks and we mitigate them and they move on to something else. And so, it's very much a cold war in that respect.

George Peabody:

Are there particular financial institution categories that you've seen as being vulnerable or being selectively targeted by hackers these days?

Robert Capps:

Hackers, fraudsters, cyber criminals, they're opportunists. They want to get as much value with as little work as possible.

George Peabody:

Well, like the rest of us.

Robert Capps:

Some call that efficient, some call that lazy. I'm not going to judge. But when you look at it that way, any organization that has value, that can be extracted by an attacker is going to be attacked as long as the amount of work that goes into it does not exceed the value taken back out. So if they can make more money flipping burgers, they will. But the sad part is that, there's just so much low hanging fruit all over the place that you as a fraudster, you don't have to look far to find potential targets or vulnerabilities that can be used to enrich yourself. And so, there's no specific vertical and financial services that's being targeted more than others. There's just areas that are being targeted more right now. So use cases who would be attractive like PDP-

George Peabody:

Yup. Actually before we-

Robert Capps:

Yeah. PDP, B2C, you name it.

George Peabody:

So before we started the recording, Robert and I were talking about Zelle. When you work with some of the banks that are participating in the Zelle Network to be able to detect bad actors knocking on Zelle door.

Robert Capps:

And a lot of that comes from understanding what happened at login, right? So if you understand there's a high risk or moderate risk at the login, understanding that that risk may continue all the way through the transaction. It's a critical decision point for allowing a transaction to go through without friction or needing to place opportunistic friction on those transactions to mitigate risk. And so, we do see organizations, financial institutions, even retailers and others that will even if

they identify that there's a moderate risk to a transact or to a login, they will allow that consumer to still interact in low-risk ways before adding friction to the interaction.

Robert Capps:

And so, they might let you look up a balance. They might look let you look at low-risk data. But if you want to transact, if you want to send money or add a payee or check out you might get, and check it and I get 3DS transaction. You might get a two-factor verification. You might get challenged in some way. Same with financial services, they might require I call the call center in some situations depending on the size of the transaction and the risk tolerance of the organization. It might be a two-factor challenge with a token that exists on your mobile device.

Robert Capps:

There's just so many different ways that organizations deal with consumer step-ups, but the key is to save those step-ups for the point where your customer needs to be stepped up versus just stepping up constantly. That challenge and fatigue has been shown to push customers away from interaction. If a customer is constantly challenged at login, when it isn't necessarily appropriate, they might think twice about logging in. And when you think about online banking, you think about retailers transactions. You want consumers to interact with those technologies as much as possible because that increases the possibility of you creating a revenue producing transaction. Yeah. And-

George Peabody:

Sure. Well, particularly in the merchant space where merchants want this as easy as possible. We've been talking in this account takeover area where there's some track record with a customer or the party that's coming in to log into the account holder at a bank. But talk to me about what you're looking at in the merchant space, in the guests checkout scenario.

Robert Capps:

Guest checkout is about how the transaction came to be, and also identifying elements within the guest checkout that might indicate safety or risk. And so, if we see a device during guest checkout that we've seen before in other guests checkouts, that might be interesting. We also see devices across our entire customer network. So maybe this transaction came from a device that has seen many, many times doing transactions at another institution or another e-commerce organization where the customer's not guest, where they're logged in and we have a good sense that that consumer is using the device during the guest checkout, that adds credibility and safety without having to influence the consumer interaction.

George Peabody:

So your customers pool, you pool on their behalf this transaction data and look at it across all of your customers.

Robert Capps:

Well, I want to be clear that we don't pool transaction data. We measure interactions on behalf of our clients, their customers. And the data that we do collect is anonymize. The data that we do collect, if it is a consumer data, it's hashed and salted so that we don't know that it's Robert Capps that's transacting. We have a global unique identifier for that data point. And we can see if that data point exists in other transactions, say for that device. And so, it isn't about having

transactional data. It's having interactional metadata about an interaction that we have to compare across customers that participate in our data consortium.

George Peabody:

Thank you. I've asked this question of other providers before, but do you have any sense of what proportion of... Well, now you've got me not wanting to just use the term transaction data. But what proportion of payment related interactions that occur on the internet, how much did that do you see?

Robert Capps:

Fair amount. I don't know whether I can give you a percentage number right off the top of my head on this one. But you have to remember that we have very large e-commerce financial institutions and other providers of value online. And so, we do see a very large percentage of align interactions on a daily basis. Yeah. And it's the very large [crosstalk 00:32:21].

George Peabody:

So let me put it kindly then that the fact that you are able to pool this anonymized data, gives you all an uplift in effectiveness.

Robert Capps:

Yeah, totally. And isn't necessarily seeing the majority of the internet, it's seeing the right portions of the internet. Having the right clients will give you a good gauge on the majority of consumers versus having to see every transaction.

George Peabody:

So if you've got the merchants that are being slammed by fraudsters, you've got the right pool, you've got the right margin customers.

Robert Capps:

Well, actually, the other way around. If you see merchants who have a large number of consumers, you have much better data. Consortium's, aren't about risk, consortium's aren't about identifying bad devices. They're about identifying good things, right? So this is a trusted device. This is a device that's seen many times transacting, good ways. It doesn't have any negative history. That's what you're looking for in a consortium because that allows you to get that customer to the transaction they're trying to complete with as minimal amount of friction and minimal amount of time.

George Peabody:

Got it. Great. Good distinction. I was being too pessimistic. So one of the things I noticed in the report that you all prepared was that the travel industry has been slammed [crosstalk 00:33:39].

Robert Capps:

Oh my gosh. Yeah.

George Peabody:

So the travel industry has been slammed by the pandemic, people aren't traveling. Or haven't been traveling anywhere near the same level they were before. What's up? Why are they getting whacked?

Robert Capps:

The percentage of good transactions is so low that there's still bad transactions happening as a portion of overall transactions. So if you actually looked at traffic volumes and checkout volumes and fraud volumes, the checkout volumes are at low, low periods, right? And then we're starting to see that lift out. As we look past the first half of the year, as we get towards, the late Summer, we definitely saw more booking volume. We definitely saw more interactions across the travel sector as countries unlocked as, some limited travel was allowed. And you even saw this just by proxy, looking at the flight schedules for a lot of the airlines were increased and they were taking plans out of mothball and putting them back in the air. And so, the legitimate volume did increase over the Summer and that sort of drowned out some of the negative stuff.

Robert Capps:

When we look at the travel industry as well, I think they were really getting hammered with chargebacks. They're really getting hammered with consumer disputes over consumers getting their money back because their flights were canceled and things like that. And so, they had like an increase in fraud transactions as a percentage of their good transactions. And then at the same time, they were having a lot of disputes with good customers. And that really became a problem for them. I think that the live event industry, concerts and theater and things like that, movie theaters, all of those industries also had a similar play out. Right? A lot of chargebacks, a lot of consumer dispute and then a mixture of fraudulent transactions in with the much lower number of good transactions. And so, there's just been a massive impact on these travel and entertainment types of veridicals from those factors.

George Peabody:

With forward sales in particular. Yeah.

Robert Capps:

Yeah. Yeah. I mean, one of my longer tenures was at the head of trust and safety risk payments and cyber crime for a major ticket resale organization. And I can't even imagine the drop-off that they've seen overnight when economies locked down, and travels probably exactly the same.

George Peabody:

Were there any surprises in what you found?

Robert Capps:

Not surprises to me, although some organizations were definitely surprised. When we look at things like e-commerce, the movement of physical transactions to virtual transactions. I think that that was a natural movement. I don't know that I would have identified the diversity of merchants being used. And so, as the normal merchants a consumer would interact with closed their physical operations, you saw people start to adopt online versions of them. So their grocery stores, ordering grocery, add deliveries, things like that. When those organizations got overwhelmed very quickly, you saw a diversification of merchants they were dealing with.

Robert Capps:

So consumer stopped dealing with merchant A B and C because they were overwhelmed, they went over to merchant E D and F. That shift was very surprising to a lot of organizations because in some cases those were much smaller merchants that didn't have a huge history with issuers. And so, I think there was a struggle with getting a lot of those transactions clear, getting them authorized because there was such a shift in consumer behavior. When we look at things like digital goods, we saw a huge increase in the number of transactions for digital goods after the lockdowns. I guess that makes sense when you start thinking about people buying new movies, games, console content [crosstalk 00:37:36].

George Peabody:

It's been good for Netflix.

Robert Capps:

And others, right. You look at all of the... Just leading up into the Christmas season, I'm not sure when this is going to get published, the holiday season for 2020, there've been a number of game consoles released to massive, massive success. Selling out wherever they go on sale, minutes later after they go on sale. That's going to translate to more digital sales as those counsels get in the hands of their users. And that's going to really drive that digital goods volume. MasterCard actually did a spending pulse report around retail sales, around across all payment types, not just credit cards.

Robert Capps:

And one of their findings recently was that 82% of the surveyed individuals said they were likely to shop online this year, much higher than previous years. In e-commerce growth, the spending pulse survey saw e-commerce growth increased 56% in October, year over year. We're going to see a lot of e-commerce transactions sort of at the detriment of brick and mortars, but a lot of brick and mortars have really blended their solutions. So they're shipping e-commerce goods directly from their stores.

George Peabody:

I was just reading an article today on how many malls have been turned into Amazon fulfillment centers, or store being used, as you say, as a fulfillment centers because the foot traffic is down. And I have to say, and I think we at Glenbrook we believe that this is going to be a permanent shift. Yes, once we get the vaccines are fully deployed and we're all back to full health, we'll still see a significant shift. Of course, people want to go shopping. They want to go out, but we're not going to return to the pre-print dynamic ratio, if you will, between in-store and online shopping.

Robert Capps:

Actually, it doesn't matter at that point when the fulfillment's happening out of the same physical big box stores that the consumer could walk into. I mean, it becomes the ultimate in very fast delivery to a consumer, when a courier can pick something up from a local store and deliver it to you versus in Amazon sending a delivery driver out the next day, or what have you. And so, it really pushes the warehouses right to the point where a customer can walk in if they don't want to deal with e-commerce so they can buy it online, have it delivered that day or maybe the next. It's a really interesting shift, that's for sure.

George Peabody:

Well, I'm not going to worry about you running out of things to do because the fraudsters are going to stay as active as ever because they too, don't want to be flipping hamburgers. And this is now organized crime, not just individuals.

Robert Capps:

Extremely organized, extremely organized and specialized. These criminals have been very good at finding their specialties and doing piecemeal work. And I think that one of the things that kind of scares me as we look at the pandemic and the impact on say the jobless rates in different countries is that consumers are now in a position where they may start taking cybercrime jobs, and almost the gig effication of cybercrime these days where legitimate job offerings, piecemeal work, gig economy work could actually be furthering some criminal activities without the consumer ever knowing, without the person ever knowing they're participating. And so, that's also a risk.

George Peabody:

Oh, man. Well, on that cheerful note, Robert, thanks so much for your time and for letting us know about what you found in the report. And will you be publishing a second half sometime in the Winter?

Robert Capps:

We're pretty good about publishing one every six months. So I would expect that we would probably see one after the first of the year.

George Peabody:

Yeah. Well, I'll put a link to the first half in the show notes, and again, really appreciate your time.

Robert Capps:

Thank you for having me.