Enhancing CX While Preventing Contact Center Fraud

Asking for more information from customers can complicate the userexperience and present new opportunities for fraudsters to hone their approach.

Introduction

It's a growing problem for contact centre managers: how do you balance customers' expectations for an efficient service while protecting them from fraud? Asking for more information from customers can complicate the user-experience and present new opportunities for fraudsters to hone their approach. More importantly, these issues may lead to reputational damage and loss of revenue for contact centres.

We live in a world of real-time connectivity. While contact centre fraud is not new, the increasing emphasis on omnichannel customer service through proactive, assisted and selfservice systems all provide new fraud opportunities – as well as increased customer expectation. Ultimately, it means more choice for both the customer and criminal.

As a result, how can you be sure that criminality won't be the cost you pay for pursuing a better customer experience through redesigned IVR and up-skilled advisors? Contact centre customer service decision-makers should be concerned about these two criminal trends:

1. Criminals are highly adaptive in their intent and are much more responsive than the average service organisation. Once one avenue of opportunity is shut down, they will find another point of access; redeploying a number of common deceptions to suit the scenario.

2. They also think differently. Their mind-set is to deceive and steal. Whereas the everyday mind-set of consumers and customer service employees is quite different: most are innocent to a potential con unless trained to spot it. Even then, conflicting objectives can be our undoing. It is desirable to go the extra mile for that upset customer who's in a hurry, blinding us to what might be really happening.

This whitepaper proposes that a deeper collaboration is needed between contact centre, customer experience, IT and security experts. From overarching objectives to effective technology, workflow and training, decision-makers must produce an open, secure and smart customer engagement strategy. The security platforms they use must meet today's expectation for real-time experience management in a world of increasing connectivity.

2. The Facts

The world of real-time connectivity has turbo-charged the level of fraud in recent years. The UK Home Secretary, Theresa May, launched a new task force in Q1 2016 as a result. Its aim is to catalyse a more coordinated response to fraud between government, industry and law enforcement. In part, this was triggered by the 2015 report from Financial Fraud Action UK. The report's main headline was that fraudsters had managed to steal £755m from British consumers and financial institutions during 2015. A 26% increase on the year before. While this number grabbed attention and stimulated a national response, the real extent of fraud probably remains understated since we do not have perfect insight into all instances.

Here, however, are some of the headline statistics:

1. The commissioner of the City of London Police, Ian Dyson QPM describes the challenge as "an estimated £30 billion cost of fraud to the UK economy"
2. An estimated 5.1 million frauds took place in the UK during 2015 (source: The Office Of National Statistics)
3. An estimated 3.8 million adults in England and Wales were victims of some form of online fraud during 2015 (source: The Crime Survey For England and Wales)
4. 112% year-over-year increases in account takeover attacks (source: NuData Security monitoring more than 18 billion user interactions cross the Internet annually)
5. Internet banking fraud rose 64% to $133m during 2015 (source: Financial Fraud Action UK)
6. £32m was lost in 2015 as a result of employees transferring funds following instructions from a "bogus boss" email. The single largest amount handed over was £18.5m! (source: City of London Police's national fraud intelligence bureau)

2.1 The Pace of Data Theft

What is clear is that we are connecting our planet faster than we are securing those connections. Considering that we have scarcely entered the era of even deeper connectivity promised by the Internet of Things and all those billions of additional points of online access, the frequency and size of ID theft caused by the current level of interconnectivity is already staggering.

> "Those large scale data breaches we now hear about today are fuelling the massive growth in downstream targeted fraud tomorrow."

The largest single data breach to date resulted in 77 million customer records being stolen via the Sony PlayStation Network. Since 2005, more than 675 million US data records have been involved in data breaches according to the Identity Theft Resource Center. In the UK, 1,163,996 UK credit and debit card records were stolen from online holiday firm Think W3 in 2004.

These data breaches provide an information baseline which fraudsters can then use to compile full profiles to either set up new accounts or plunder existing ones. In other words, those large scale data breaches we now hear about today are fuelling the massive growth in downstream targeted fraud tomorrow. A recent test to determine the speed at which compromised data travels discovered the following: It took just 12 days for the account information of 1,500 "employees" to travel from California to 22 countries and five continents. In the first few days, the information was viewed over 200 times and in 12 days over 1,000 times. In comparison, it takes an average of 205 days for most organisations to detect a breach has taken place.

2.2 Gauging the Impact on UK Contact Centres

How much the contact centre industry directly suffers as a result of fraud is unknown. All that can be inferred about its extent comes from a number of sources. • Official statistics that show increased levels of fraud

- Regular alerts published by organisations such as Financial Fraud Action UK who publicise latest fraud techniques that include contact centre crime
- Evidence gathered by contact centre fraud vendors such as Pindrop who have published what they know using aggregated research from their own clients

While any contact centre is a potential fraud target, some sectors such as retail and financial services are closer to the eye of this storm and draw more attention from fraudsters. Thus Pindrop's research is exclusively drawn from financial service clients. This is what they know:

- 1 in 700 UK contact centre calls to financial service organisations is fraudulent (compared with 1 in 1,700 in the US)
- £0.51 is lost to fraud on every UK call (the US equivalent is £0.40)
- 45% growth is the rate of fraud for US financial service clients between 2013-15

2.1 The Pace of Data Theft

What is clear is that we are connecting our planet faster than we are securing those connections. Considering that we have scarcely entered the era of even deeper connectivity promised by the Internet of Things and all those billions of additional points of online access, the frequency and size of ID theft caused by the current level of interconnectivity is already staggering.

> "Those large scale data breaches we now hear about today are fuelling the massive growth in downstream targeted fraud tomorrow."

The largest single data breach to date resulted in 77 million customer records being stolen via the Sony PlayStation Network. Since 2005, more than 675 million US data records have been involved in data breaches according to the Identity Theft Resource Center. In the UK, 1,163,996 UK credit and debit card records were stolen from online holiday firm Think W3 in 2004.

These data breaches provide an information baseline which fraudsters can then use to compile full profiles to either set up new accounts or plunder existing ones. In other words, those large scale data breaches we now hear about today are fuelling the massive growth in downstream targeted fraud tomorrow. A recent test to determine the speed at which compromised data travels discovered the following: It took just 12 days for the account information of 1,500 "employees" to travel from California to 22 countries and five continents. In the first few days, the information was viewed over 200 times and in 12 days over 1,000 times. In comparison, it takes an average of 205 days for most organisations to detect a breach has taken place.

2.3 The Customer Response to Fraud

> "Brands are blamed and shamed for failing to protect customers from fraud when it happens."

A 2015 UK study by contact centre experts Compliance3 shows the behavioural impact on customers once they become fraud victims. The findings drum home the extent of both economic and reputational losses on the affected brands. Of which the actual losses are just the tip of the iceberg.

- 41% blame the brand while 30% blame the payment card company for the fraud happening
- 70% state that payment card fraud would seriously impact their future purchasing behaviour with 4 out of 10 saying they would never buy from the brand again
- A further 27% would avoid the brand 'for a while', leaving those consumers open to competitive offers
- 85% of fraud victims would tell someone about what had happened of which 16% would take to social media to amplify their story

In the context of customer experience ambitions this makes terrible reading. Brands are blamed and shamed for failing to protect customers from fraud when it happens.

Alarmingly for brands, 40% of defecting customers' future lifetime value is lost forever. Nearly 30% of short-term customer revenue is lost with some of those customers probably leaving forever. In addition is the impact of reputational damage based on word of mouth. This is harder to quantify, but is likely to ripple through each victim's personal network and, possibly, beyond given today's use of social networks to file a complaint.

41%

blame the brand

30%

blame the payment card company for the fraud happening

70%

state that payment card fraud would seriously impact their future purchasing behaviour

4 out of 10

saying they would never buy from the brand again

27%

would avoid the brand 'for a while' leaving those consumers open to competitive offers

85%

of fraud victims would tell someone about what had happened

16%

would take to social media to amplify their story

3 As Fraud Gets Bigger, Brands Must Get Smarter

> "As contact centre managers, we need to think about this ingenious invasion of our service ecosystem in equally sophisticated ways."

Fraudsters adapt and learn, and the simple truth about any form of security is that a locked door is compromised whenever other doors are opened. As of now, the contact centre is an open door. This customer touch point currently remains the most vulnerable for a number of reasons:

1. The dominant approach to authentication and verification needs reinventing. It is timeconsuming, confusing for genuine customers and pretty much ineffective against professional criminals. Traditional KBA (knowledge-based authentication) uses personal information that fraudsters can easily discover or purchase in today's world. Rapid adoption of biometricbased authentication is an industry priority.
2. Advisors can be persuaded to 'open the door'. This paper explores how this happens and what can be done in more detail later on.
3. IVRs are now being used as fraudsters' 'test and learn' environments to complete profiles, authenticate them, take over accounts or issue instructions that then allow them to complete the intended fraud in another channel. We need ways of being alerted in real time to those patterns of illegal behaviour. IVRs have remained out of sight/ out of mind for operational leadership for too long.
4. Text channels are being hijacked. We all receive those persuasively branded emails and text messages from our banks to act now for some urgent reason. We might bin them, but how many less savvy people fall prey?

As contact centre managers, we need to think about this ingenious invasion of our service ecosystem in equally sophisticated ways:

1. We should be educating ourselves about the fraudsters' journey in much the same way we think about customer journeys.
2. How and when is the contact centre involved in this broader activity? We should be mapping and updating it in the same way we track our constantly evolving customer experience.

3.1 Potential Risk Scenarios

To understand how and when fraudsters might impact contact centres, imagine these different scenarios. For example, the criminal might start by completing a personal profile with a voice interaction via the contact centre and then move onto the online channel to actually commit the fraud using that information to initiate transfers, withdrawals or payments. In another very real situation, fraudsters could begin with direct consumer contact, using a fabricated urgency to persuade them to reveal personal details such as a PIN number. Armed with this, the fraudster can then drain the victim's account via IVR access.

Another version – this time focussed on banking customers – starts with a text, letter or email that appears to be from the customer's bank. They are asked to make contact via the provided phone

number. The fraudster redirects the call to the actual bank and records the conversation, noting the victim's security answers and personal details. These are then later used to commit the fraud. The reason why this scam is so successful is because the fraudster's presence is unknown to both the victim and the bank.

> "Visualising these activities as joined-up journeys helps us understand what is happening"

Visualising these activities as joined-up journeys helps us understand what is happening. Let's also consider how much more complex these scenarios will become as we expand our omni-channel ecosystems. Every service organisation is currently figuring out which of the following options makes up their ideal channel mix.

We also know that the channel mix changes each year as customers' online behaviour evolves. Just look at the recent growth in messaging apps, strongly suggesting they will become a significant service channel in the near-term future

3.2 The Responsibility to Protect Contact Centres

Contact centre fraud requires broader understanding of what is happening both upstream and downstream. We must recognise it is part of today's contact centre leadership duties to ensure the required time and resources are invested into keeping track of where the contact centre fits into the full fraud scenario.

It also requires an awareness of how individuals within the contact centre can be compromised into adding those final details which allow a fraudster to act.

Being conned like this is now called social engineering. In other words fraudsters manipulate their victims into sharing confidential information. Sometimes it happens on an ad-hoc basis. Other times, fraudsters are patient and prepared to play the long game in gaining those final pieces of personal data. Here's a scam reported by the UK's National Fraud Intelligence Bureau's Proactive Intelligence Team during summer 2015.

Customer services staff were being befriended during their days off and "groomed" by fraudsters over long periods of time in order to gain access to personal account data. Typically the fraudsters exploited the staff member by either offering a financial lump sum for the account information or by exploiting disgruntled, unhappy staff. One bank employee ended up in jail as a result.

As a contact centre leader you should be aware of this potential grooming threat and embed discussion about it into inductions and team briefings: the lesson being that whenever teams congregate locally and can be recognised, there is potential danger.

4. Where Contact Centres Need to be Guarded

Let's now think a little deeper about the core vulnerabilities we need to protect ourselves from. I'm going to explore three of the most common scenarios in an omni-channel set-up.

4.1 Live Assistance

In a live assistance context, the fraudster will use what they already know to convince the advisor they are a real customer to gain more of the profile data they still need in order to pass other security measures later on.

In this phase they are collecting, testing or adding to what they already know. Sometimes they will use the opportunity to change customer profile data to their advantage. Maybe next time they can persuade the advisor to 'do the right thing' and mail a new card to that recently changed address they now control.

Pindrop research has identified that in this phase of the fraudster's journey, they typically make up to five calls before asking for money. This strongly suggests we should be tracking them during this upstream phase.

They will also keep calling back until they reach the type of advisor they can manipulate. Probably someone less experienced; certainly someone who tends to respond with their heart rather than their head. To them, it would have felt like an authentic customer need. What do you do when you want to win that advisor-ofthe-month award and you hear "I'm stranded and my PIN isn't working?" Innocently, you might consider it a perfect opportunity to shine.

Outside this ongoing opportunity to defraud, sometimes it's a deliberate manipulation of circumstances. Let's imagine the contact centre is being overwhelmed with an unexpected spike in inbound contact.

It could be for negative reasons such as a service failure that is still disrupting huge numbers of customers. It could be positive reasons such as interest in a massively successful product launch. Regardless, we can thank social media for delivering that breaking news which anyone from journalist to fraudster can tap into.

The event could even be engineered by fraudsters themselves by initiating a so-called distributed denialof-service attack (DDoS) in the online channel in order to flood the contact centre channel. These attempts to choke a communication channel by flooding it have also been reported in the telephony and mobile SMS channels.

Whichever way, the contact centre is now on the back foot and under-resourced, creating chinks in normal security best-practices that fraudsters can exploit.

It could be a time when standards around knowledgebased authentication can be dropped in favour of speeding up the call. Gartner report that 10-30% of genuine customers fail on some aspect of KBA anyways (source: Gartner: When Knowledge Based Authentication Fails 2012). Fraudsters are aware of this, flooding contact centres at such times of vulnerability to gain that extra piece of information they are seeking.

4.1.1 The Technology They Use

> "Too much conformance kills the instinct to do what matters in the moment."

In terms of deepening our understanding of why these fraudster journeys succeed, it is also important to be aware of the technology being used and how it can be engineered to fool us.

An encrypted messaging app, for example, can be used for both 'good' and 'bad' reasons. So too with internet carried conversations (VoIP services) and call ID masking services. Let's look at each in some detail.

Since a VoIP carried conversation is split up and distributed over the internet's many carrier networks, it is very hard to figure out the true origin of that call. According to Pindrop's research, VoIP based fraud is a much larger issue for US organisations. For them, 52% of contact centre fraud originates off-shore versus 28% here in the UK which is nonetheless four times higher than legitimate off-shore calls from genuine customers. Dovetailed with this fraudsters' journey is the higher use of VoIP services. 46% of US contact centre fraud is committed via VoIP. Here in the UK where domestic fraud is much more prevalent (72% of all fraud), VoIP use is less common (22%). Instead mobile fraud is the communication channel of choice in 64% of instances. While we are seeing a steady increase of smartphoneoriginated calls instead of traditional landlines within everyday contact centre trends, Pindrop point out that mobile access is still proportionally greater in fraud than normal use. Here's why:

1. ID masking: It is easy to find an app to do the job. Of course there are legitimate use cases. For instance, it could be making an international business look like it has a local presence. But equally it could be used to mask a call from an African or Eastern European fraud gang.
2. Unknown caller: Another tactic is simply changing the setting on your smartphone to completely hide your number and become an unknown caller. The popularity of this approach is reflected in the fact that 70% of UK fraud calls use a restricted caller ID (source: Pindrop).
3. Pay-As-You-Go: Low cost of disposable 'pay as you go' phones, combined with number altering and even voicealtering apps, means the fraudster has every opportunity to stay ahead.

52%
52% of US contact centre fraud originates off-shore

28%
28% of UK contact centre fraud originates off-shore

46%
of US contact centre fraud is committed via VoIP

72%
of UK fraud is domestic

22%
of VoIP is used in of UK fraud cases

64%
of mobile fraud instances in the UK is mobile fraud

4.1.2 How Do Contact Centres Develop Effective Counter Measures?

> "Too much conformance kills the instinct to do what matters in the moment."

Ignoring the opportunity that smart technology offers for a moment, keeping vigilance within the advisor and team leader communities is a challenge. We know from regulatory environments that complianceinspired behaviour is often at odds with customer experience agendas. Too much conformance kills the instinct to do what matters in the moment. There remains a fine line between being blamed for typical 'non co-operative contact centre behaviour' and being seen to step-up and help when genuine customers are in need.

To that extent, scenarios need creating based on both the ones described here and those readily available on an ongoing basis from organisations such as Action Fraud UK (http://www. actionfraud.police.uk/). Advisors then need to be provided with engaging ways to improve their acuity and awareness of fraudulent behaviours.

We have to recognise this truth. Contact centre people are orientated towards helping other people and delivering a customer experience agenda which becomes ever more challenging. They can help, but are not in pole position as the solution.

Instead, technology has to be used to do the heavy lifting. Moreover, to avoid a clash of agendas, the security shield has to act as an unobtrusive 'silent guardian' in the background which can react in real-time and keep the advisor, customer and brand out of harm's way.

One thing that is slightly to our advantage is that – from the fraudster's perspective – working through live advisors presents a risk. Some may notice a pattern of repeated calls. The more experienced may report instances of probing as potential fraud. For these reasons, self service via IVR remains a safer option.

4.2 Voice Self Service

> "Too much conformance kills the instinct to do what matters in the moment."

The scope and value of fraud opportunities depends on the type of IVR service you run. In the financial service sector, Pindrop research shows IVRs receive as much attention as the live assistance channel this suggests the pickings are rich. From the fraudster's point of view, IVR remains a favoured point of access. It's impersonal, automated and, in many cases, not monitored for patterns of fraudulent behaviour.

From the brand's perspective, self service is a priority in today's world of 24x7 access. Hence many IVRs are being augmented with natural language interfaces and functionally extended to offer personalised access to information and transactional services.

What is typically missed in these technology refreshes is an enriched security layer able to pick out fraudulent patterns of behaviour and bring them to the right people's attention. Meanwhile, IVRs provide criminals with an unnoticed opportunity to validate

information they already have and probe for additional information.

For instance, if they have an account number and a date of birth, but no PIN, they can repeatedly call into the IVR to try and guess the right combination with little risk of being noticed. Unfortunately, this yields results since too many people still use obvious numbers such as birth dates for PINs. Once they have gathered PIN numbers, they will look for the most convenient automated process, often the IVR itself to try and use the information they've collected to their advantage.

If it's a financial services brand, they can use its IVR to check balances and any pending deposits to figure out when the most lucrative time to clear the account will be. Alternate strategies might be to purchase something online or over the phone (known as a "card not present" transaction), create a counterfeit card or alter an account address then request a new card is sent to that address.

By the way, it's worth noting that in the last example, the way in which UK houses are typically converted into flats makes this a much easier fraud opportunity than in the US. Unlike US buildings which tend to offer lockable individual mailboxes in public hallways, UK flat owners typically collect their mail from a communal pile. This makes it much easier for a fraudster to intercept.

The message around IVR fraud is that we lack insight and real-time responsiveness. This provides a haven for criminal activity. If any IVR journey directly or indirectly provides access to personal information about a customer, then assume it can be stolen or altered for the purposes of fraud. If your IVR has payment capabilities then the risks are even greater.

4.3 Proactive Service

One of the mantras of customer experience is to design frictionless engagement. The notion that reducing customer effort is more valued by customers than being delighted has also been a well debated topic in recent years. An all-encompassing mission has developed from these ideas to make customer journeys simpler, redesigned around customer priorities. In a contact centre context this often translates into a push for more proactivity. If we have a high level of certainty that customers are going to make contact, surely it is smarter to anticipate that demand and make contact before they need to. In a world gone mobile, the obvious way to do that is via SMS.

As customers we love:

- Being reminded about a heath appointment
- Being told when to expect a home delivery
- Being advised that a desired item is back in stock
- Being alerted to an unexpected incident

In fact, we now expect it. And this creates opportunities for the fraudster. Here is a real example.

Many of the messages used for proactive customer communication are automated, triggered by an enterprise workflow. These are called 'Application to Person' or (A2P) messages. Fraudsters can now mimic those A2P messages if there is a weakness in the mobile carrier's network.

They use specialist software which alters the sender ID on the message to become the same SMS ID that the brand uses. The software is smart enough that the phishing text can even become included within an existing message thread on the customer's phone for additional credibility about the sender's identity

The scam text messages typically claim that there has been fraud on the customer's account or some kind of urgency (i.e. a failed payment or a previously unknown direct debit) requiring authorisation. Anything, in fact, that emotionally provokes someone into hasty action.

> "One of the mantras of customer experience is to design frictionless engagement."

The texts then encourage people to call a number or visit a website. You can guess what is meant to happen after that.

Even before we have leveraged the full benefits of proactivity on customers' behalves, the goodwill which this ought to generate is already being soured with understandable suspicion about the authenticity of these communications. Fraudsters learn fast.

5 Initial Conclusion

> "The right solution for this needs to be adaptive. Both the art of customer experience and that of fraud will continue to dynamically evolve."

Contact centre managers now need an approach that knits together customer experience and security management. Secure, low-effort engagement for the customer is the desired outcome. The ideal customer value proposition is that it is both easy and safe to do business with your brand. This means the client can trust you to keep their identity and money secure.

The right solution for this needs to be adaptive. Both the art of customer experience and that of fraud will continue to dynamically evolve. The customer experience is what we feel and notice while the security remains invisible.

Since fraud is a multi-step journey, this solution must aim to recognise upstream activity as soon as possible. Ideally it should help track those fraud journeys and point out where stronger defences need building. Recognition of criminal intent has to be real-time, actionable insight, embedded into a workflow that allows specialist teams to then rapidly secure a breach and ideally identify the perpetrator.

6 Discovering a Complete Strategy

> "The right solution for this needs to be adaptive. Both the art of customer experience and that of fraud will continue to dynamically evolve."

An effective solution will comprise a number of elements that need organising into a coherent strategy and detailed plan. This then needs to be adequately resourced and managed as a collaborative effort amongst stakeholders.

Key elements of your strategy should include:

- A unified approach that secures the entire ecosystem of customer touch points as well as the unique challenges of each individual touch point
- A multi layered approach to security technology (e.g. voice biometrics plus Phoneprinting ™)
- Recognition that omnichannel contact centres need both text and voice surveillance (ideally integrated)
- The ability to track both live assistance and self service (eventually covering voice calls, chat, IVR and intelligent assistance)
- Active participation with national security agendas for improved responsiveness
- The visualisation of fraud journeys affecting your brand to improve internal understanding
- A trackable programme of education for staff and customers
- A communication and compensation strategy in

7 Final Points

> "Rather than pretend it isn't happening, brands should be amplifying the efforts of national agencies by helping to educate their customers."

In the online world, copycat websites, fake emails, and offshore phone calls continue to tempt customers into losing out. Rather than pretend it isn't happening, brands should be amplifying the efforts of national agencies by helping to educate their customers.

It is about maintaining awareness around the basics.

- Teaching them how to spot a fake approach.
- Warn them of the latest scams.
- Show you are committed to their safety.

Finally, Pindrop's continued pursuit to support contact centres and identify areas of vulnerability is vital. Its Phoneprinting technology and support services should be explored as they are at the forefront of contact centre protection against fraud.

Protecting Customer Experience While Controlling Contact Centre Fraud

About The Author

Martin Hill-Wilson is a long term contributor to the UK contact centre market. He is a well known keynote speaker and chair at industry conferences. He also runs numerous master classes on customer engagement and service design. He was awarded industry lifetime achievement awards in both 2014 and 2015. More about Martin can be found at www.brainfoodextra.com.

Footnote

I'd like to thank Glenn Hurley,
CEO of Compliance3
www.compliance3.com
for his kind permission to use their research in this whitepaper.