

WHITEPAPER

Social engineering

The psychology of scams, and how technology can prevent them

Contents

Fraud costs the global economy
\$5 trillion each year

Sophisticated scammers

But whose responsibility is it?

Why won't they listen?

So what can be done?

Education

Friction

Nudges

Data

Where do we go from here?

4

5

6

7

10

11

13

14

15

17

About the authors

This paper was written by Nick Padmore and Richard Shotton from [language and behavior consultancy Schwa](#).

Nick is creative director, and focuses mostly on the language side. He spends his time helping organisations of all shapes and sizes to write more clearly, empathetically and persuasively.

Richard is a behavioral scientist and author of The Choice Factory, a best-selling book on how to apply findings from behavioral science to advertising. He tweets about the latest social psychology findings from the handle [@rshotton](#).

SECTION ONE

Fraud costs the global economy \$5 trillion each year

That's around \$700 out of the pocket of every person on the planet. And according to accounting firm Crowe, [who came up with that number in 2019](#), it's only getting worse.

A big reason for that is that banks' and retailers' customers have been steadily moving towards being exclusively online – a trend that the COVID-19 pandemic has only exacerbated.

The poisoned chalice

The internet opens up countless opportunities for organizations to offer slick, friction-free services that give customers more control over their money. But it's also a prime culprit for the stratospheric rise in the amount of money being lost to fraudsters on a daily basis.

While big banks and retailers have the means to spend billions on security and put processes and procedures in place to mitigate risk, the public is largely oblivious to the dangers that lurk in the shadows. And those dangers are only growing more and more complex and refined.

SECTION TWO

Sophisticated scammers

We spoke to fraud experts from a group of global banks and retailers including Hello Fresh, MobilePay, Nordea, Santander and Wells Fargo to get their take on the issue.

All of them agreed on one thing:

“Detecting and preventing scams is hard. Really hard.”

Million-pound scams are few and far between. Criminals know that if they chip away at the bank balances of everyday people, they can fly under the radar. These low-value transactions are harder to detect, both from the perspective of banks and retailers, and of the victims themselves.

Scammers even coach their victims to navigate warning messages and security measures. So on the off chance that the scam does raise an alarm, it's still an uphill battle to convince the victim not to let it happen.

As a result, the problem is reaching pandemic levels. In the UK, the Royal United Services Institute even recently went as far as to say it's a **"national security threat"**.

“Low-value card transactions are very difficult to prevent. They're not using secure channels, and the vast majority of scams involve customers making the payment themselves. That's the core, core challenge.”

Head of Fraud Strategy (Banking)

SECTION THREE

But whose responsibility is it?

That seems a surprising amount of accountability for people to take on. And there's an argument that puts responsibility entirely in the other camp: it's banks' and retailers' services criminals are defrauding, so it's down to them to do something about it.

The reality is that both sides have a part to play. When you buy a car, you expect the manufacturer to have installed airbags and good brakes, but it's also your job to drive safely.

So what stands in for airbags and brakes when it comes to preventing fraud and scams? Education, education, education. Banks and retailers spend a lot of time and money on campaigns to raise awareness about the dangers, and most of the major players drop warnings directly into the user journey too.

Some have gone even further and started offering compensation. In the UK, the PSR (payment services regulation) sets to reimburse victims of scams and fraud.

The sense we got from our interviews was that a lot of the good work organizations are doing is falling on deaf ears. One bank we spoke to even said they didn't send warnings at all, because most ignore them, and those who don't just get overwhelmed, scared or confused.

The results of our survey back up these comments too.


We found only 50% of consumers can recall seeing a message warning them of a scam when making a digital bank transfer. That's a bad sign, particularly as our sample was entirely made up of people who said they do bank or shop online.



SECTION FOUR


Why won't they listen?

If detecting scams is hard, getting millions of people to listen to and remember educational messages is even harder.



An empathy gap
When people see the warnings and advice they're in what psychologists call a 'cold' state: calm, dispassionate, bored. But when they're actually at risk, they're in a 'hot' state: emotional, stressed, angry.

When we're in a cold state, we struggle to imagine how we'll behave in a hot state (and vice versa). So when we're calm, it's more than possible that we'll read a scam warning and make a mental note to be careful. But when the scam is in progress and we're stressed, all that preparation goes out the window.



Complacency
We tend to overestimate our own abilities.

In a 2019 study, psychologists from New York University recruited 464 participants and showed them eight phishing emails. Half of the participants had to predict the likelihood that they'd follow the instructions in those emails (like clicking on a dubious link). The other half had to predict the likelihood that a typical participant, of the same

age and gender, would follow those instructions.

Backfiring incentives
When a Munich taxi company installed anti-lock braking systems in half their fleet, they might have expected that half to be involved in fewer accidents. But over a three-year experiment, that didn't happen – in fact, the taxis fitted with ABS were involved in slightly more accidents.

This is down to **risk homeostasis**: the harder you work to protect people, the more risks they take.

Let's take stock for a moment. Fraud and scams are on the rise. People are incentivised not to worry too much about avoiding them. And the more banks and retailers do to protect their customers, the more risks those customers take.



Fig 2. How easy it is to avoid online fraud?
70% think it's easy to identify if an SMS text message is a scam



“

Fraud and
scams are on
the rise. People
are incentivised
not to worry
too much about
avoiding them.

”

SECTION FIVE

So what can be done?

Risk analysts use something called the Swiss cheese model, which argues that the best way to protect against risk is to put as many barriers between it and the potential victims as possible (like slices of cheese).

The idea is that if the threat manages to get through a hole in one slice, there's another slice there to stop it going any further.

Right now, there are plenty of slices standing between customers and scammers: but if a criminal dupes a customer into legitimately transferring their money, those slices melt away. So in truth, there's only one slice: education. It's an important barrier, but it should be part of the solution rather than the whole solution.

There's a great deal more that can be done, and we've organized the tools into these four categories:

1



EDUCATION

2



FRICTION

3



NUDGES

4



DATA



EDUCATION

We've talked about how attempts to educate customers often fall on deaf ears. But the problem isn't with education per se – it's a powerful tool – it's with treating education as the be-all and end-all.

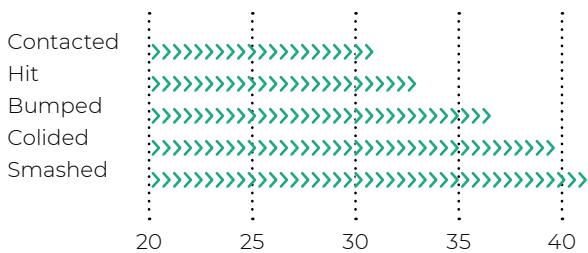
It's vital that the industry continues to educate customers about the risks they face when making online transactions. And with a little behavioral savvy, it's possible to make these campaigns and comms really resonate.

For instance, scaring customers with huge numbers about the magnitude of the problem might not be the most effective way to get their attention. The **identifiable victim effect** tells us that people are much more likely to be moved by the story of a specific victim instead. So it might pay to focus on just one person in your next campaign, rather than millions.

The language you use can have a huge impact on how successful your communications are too. Think about the difference between a burger that's 90% lean, and one that's 10% fat. They're the same burger, but one sounds much more appetizing than the other.

In 1974, psychologists from the University of Washington **found that the way they framed a question had a significant impact on the answers they got**. They had people watch seven films of traffic accidents, and asked them how fast the cars were going in each case.

HOW FAST WERE THE CARS GOING WHEN THEY...?



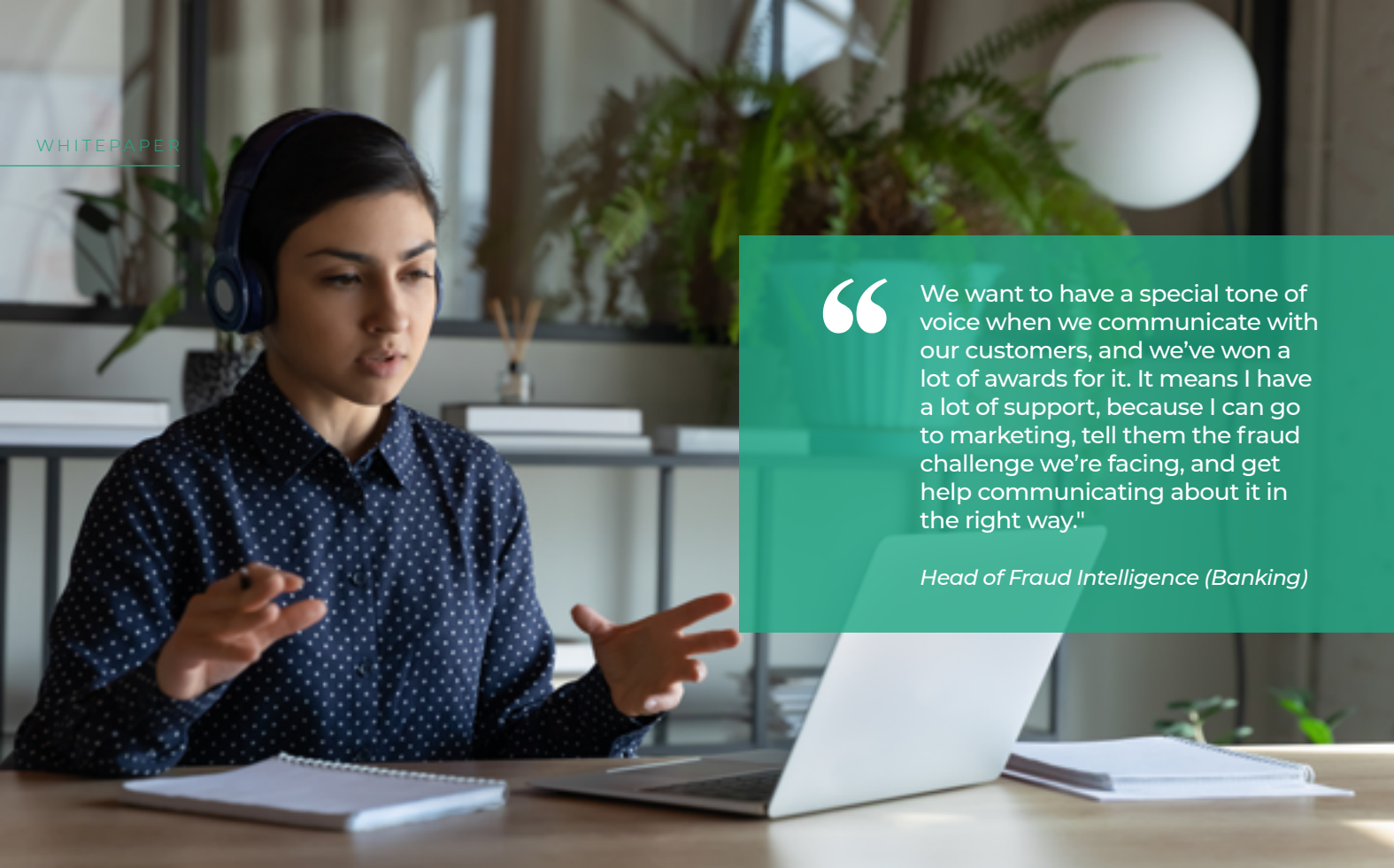
Those who were asked 'How fast were the cars going when they contacted each other?' estimated much lower speeds than those who were asked the same question, but with "smashed" instead of "contacted".

This means if you want people to stop and listen, every word you choose counts.

There are, of course, plenty of businesses out there that have defined their tone of voice, and use language both to stand out from their competitors and build empathy with their customers.

But they're the exception, rather than the rule.





“ We want to have a special tone of voice when we communicate with our customers, and we've won a lot of awards for it. It means I have a lot of support, because I can go to marketing, tell them the fraud challenge we're facing, and get help communicating about it in the right way.”

Head of Fraud Intelligence (Banking)

One of the fraud experts we spoke to told us about the "lingo bingo" approach banks often take to communication. Buzzwords, jargon and cold, corporate terminology can all stop customers from reading the warnings put in front of them, and even make them **think worse of the people behind the communication**.

So assuming you've framed your message in the right way, and it's as clear as can be, the other thing to think about is how to make it memorable.

Behavioral scientists talk about the **Von Restorff Effect**, which suggests we notice and remember things that are distinctive.

It's likely, for instance, that you won't remember every point we've made in this paper, but you probably will remember that there was a picture of a pineapple right in the middle.

All of this means no matter how well a warning message might work, the effect will start to wear off the more people see it. It's crucial, then, to keep refreshing these messages and, for the bolder organisations

out there, to attempt to make them sound a little different to what people might expect. A clever or intriguing headline, for example, might well have a bigger impact than a functional one.

Concrete language can help with memorability too. In a famous experiment from the 1970s, Ian Begg discovered that **we're three times more likely to remember concrete phrases** like 'white horse' and 'muddy village', compared to abstract ones like 'subtle fault' and 'absolute truth'.

Begg's hypothesis was that the concrete phrases paint a picture in the mind, whereas the abstract ones don't. In the context of scams, this suggests it's more likely people will remember a warning to "keep an eye on your money" than one that asks them to "remain vigilant".

FRICTION

Small, seemingly inconsequential barriers have a disproportionate effect on the way people behave. Nobel laureate Daniel Kahneman argues that the most effective way to change behavior is to either remove, or add, these barriers.

In 1998 the UK government ruled that paracetamol should be sold in quantities of no more than 32. So anyone who wanted more would need to go store to store.

That little bit of added friction has led to around 43% fewer paracetamol-related deaths, and a 61% drop in requests for liver transplants due to paracetamol poisoning.

Also in the UK, the Behavioral Insights Team got **36% more people in large organisations to take up a workplace pension**, just by switching the default from 'opt-out' to 'opt-in'. In this case, the impact came from removing friction: all people had to do to enroll was nothing at all.

One of the biggest bits of friction that stops people heeding fraud warnings is when the message arrives. We mentioned earlier that these messages tend to sit at the very start of a user journey, when customers are in a cold emotional state, and that by the time a scam is in progress all the advice has been forgotten.

The key is timeliness. You have to get the message in front of people at the exact moment they're in danger; when they're in a hot state.

It's worth looking at your own user journeys and thinking: where can I add or remove friction to help people stay safe?



“ We can educate till we're blue in the face. The only thing that works is telling customers exactly what to do at the exact moment they need to do it.”

Head of Fraud Strategy (Banking)

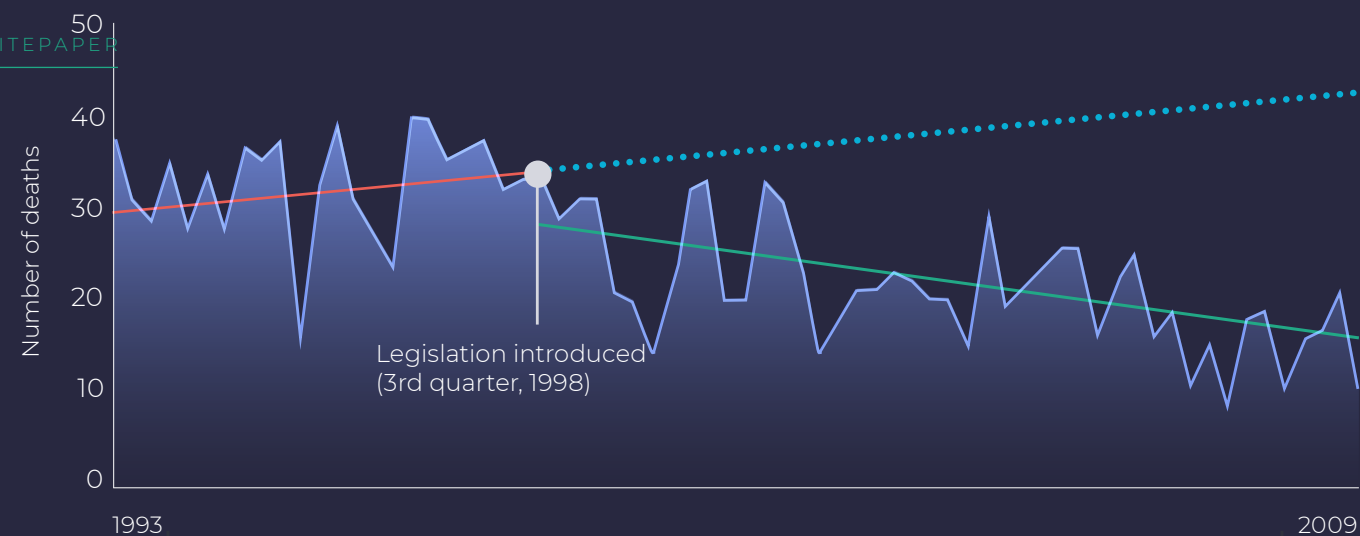


Fig 3

In 1998 the UK government ruled that paracetamol should be sold in quantities of no more than 32.

— Trend before legislation
 Predicted deaths based on pre-legislation trend
 — Trend after legislation



NUDGES

In 2008, economist Richard Thaler and legal scholar Cass Sunstein published the book "Nudge", and a new movement was born. The book walked through the ways it's possible to indirectly influence the way people behave, for their own good.

A lot of the case studies in this paper have involved nudges, from making workplace pensions opt-in by default to limiting the size of paracetamol packs.

And there are many, many more examples to draw on.

Like giving a 'because'. **According to this famous study**, the word 'because' has special persuasive power. So if you want to stop someone transferring some money, or giving away their details, or anything else that could harm them, don't just tell them not to do it. Give them a reason not to do it.

There's also a fascinating principle known as the **Keats heuristic, or rhyme-as-reason** effect, which states that people are more likely to believe a phrase that rhymes compared to one that doesn't.

Think 'An Apple a Day Keeps the Doctor Away' and 'East or West, Home is Best'. A final point we'll make here is about visual congruence. It's not just the way you frame your language in a warning message that impacts whether people will heed your advice; it's the way it looks too.

In 1991, an academic from New Mexico State University looked at **how the color and shape of warning labels influenced whether people complied with them**, and found that red, octagonal labels worked best.

Of course, there are big challenges around color for banks and retailers. For those brands with a lot of red in their visual identity, its effect in warning messages might be reduced, so our recommendation would be to test a variety of options and see what works best. And for the brands with little or no red, the main issue is likely to be getting the brand team engaged. That's a trickier one to solve, and it will vary from company to company, but it's a matter of weighing up the relative dangers to the brand and to customers, and breaking down internal siloes so that everyone's got the same goal (more on that later).



DATA

Small, seemingly inconsequential The ideas we've presented so far have focused on prevention, rather than detection. But the holy grail here has to be both: if you can detect when a customer is in trouble, your efforts to intervene and prevent them becoming a victim will be infinitely more powerful.

These interventions have to be dynamic. If a swimmer gets into difficulty in a pool, the lifeguard doesn't just point to a disclaimer saying 'Enter pool at own risk'. They're always there, watching and waiting, looking for clues that someone's in trouble. And when they see the clues, they dive in and help.

With scams, the clues are hard to spot. But they're there if you look in the right places.

For instance, **Callsign's** dynamic interventions software will check the user's device for malware and other threats, and look for anomalies like an unusual location, or odd behavioral patterns. Those behaviors could be typing one-handed, moving the mouse strangely, or taking a while to click or tap through an online form, all of which would suggest they might be on the phone to someone who could be trying to socially engineer them into handing over money.

And there's an extra benefit to this too: if you can detect scams as and when they're happening, your warning comms can be targeted so that only the people who are genuinely at risk will see them. That way you eliminate the 'crying wolf' effect that comes with a blanket approach to communications.



“This is a very 21st-century problem, and the only way to win is to take a very 21st-century approach to fighting back.”

SECTION SIX

Where do we go from here?

We're confident that the ideas we've outlined give banks and retailers a chance to get on top of this digital pandemic.

But what we're absolutely not saying is that every idea will work every time. The key is to test and improve ad infinitum, rather than to set an agenda and stick with it come what may. And to **build your approach based on the Swiss cheese model, with more barriers rather than fewer.**

Dynamic interventions does it all automatically. It's powered by data, so it only acts when it believes someone to be at risk. **It adds the right level of friction, without slowing down people doing legitimate transactions. And it uses clever nudges to stop people in their tracks, with language companies can tailor to their own tone of voice.**

It'll also help with that lesser-discussed vital ingredient in the war against scams: teamwork.

If fraud teams and customer experience

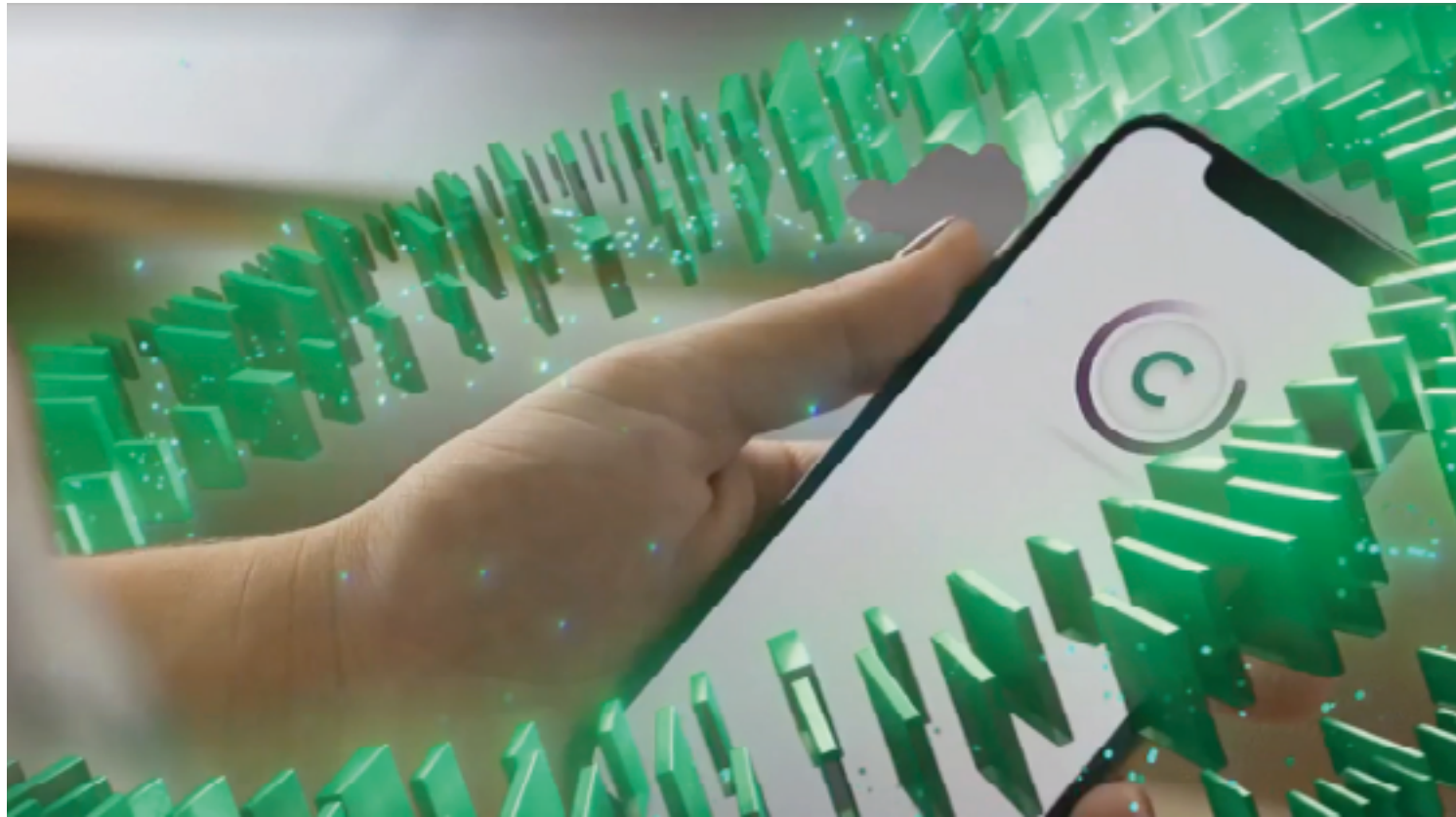
teams pull at opposite ends of a rope in a game of corporate tug of war, nobody's going to emerge as the winner.

Both groups have a vital role to play. Fraud teams know the extent of the danger, and how to fight back. Customer experience teams have an insight into the minds and behaviors of their users, and what's likely to help or hinder them.

A successful strategy for battling fraud and scams doesn't just involve using the ideas in this paper. It means breaking down some of those corporate walls, and having fraud people and customer people working side by side, rather than at odds with one another.


This is a very 21st-century problem, and the only way to win is to take a very 21st-century approach to fighting back.







THE ANTI-SCAM SOFTWARE WITH BEHAVIORAL SCIENCE BUILT IN

This paper was commissioned by Callsign, the digital identity pioneers.
Their dynamic -interventions software takes a three-part – Detect, Intervene, Protect – approach to tackling scams:

- 

Detect – real-time ATO and scam detection
Callsign analyzes more data points than any other solution on the market across threat, device intelligence, location, and our unique Muscle Memory Technology – the highest-fidelity form of behavioral biometrics.
- 

Intervene – cross-channel dynamic fraud messaging based on real-time intelligence
Whatever the threat, Callsign stages the right intervention, every time. When it comes to social engineering, Callsign's hyper-personalized messages are contextual and effective. By asking the right questions at the right time, Callsign eliminates the predictability of static warnings, providing dynamic questions that scammers can't anticipate – or coach their victims through.
- 

Protect – safeguard long term business reputation with non-repudiation
With Callsign you can apply dynamic policies that adapt in real-time to request additional actions from the customer or block payments. Non-repudiation is covered with full audit capability and journey visualization.

Callsign lets you deliver seamless experiences and greater security at a lower cost, whilst ensuring that your genuine customers can get on with their digital lives.

callsign[®]

Balancing security, UX & privacy is easier than you think.
Find out how we can help you on your journey to digital leadership – callsign.com.

Get in touch for a demo of our capabilities: sales@callsign.com

© 2022 Callsign Inc. All rights reserved.