White paper
Security and Biometrics

How social disruption drives contact center fraud

And how to fight back, with stronger identity and credibility checks.

By Simon Marchand, CFE, Adm.A.
Chief Fraud Prevention Officer, Nuance Communications

Contents

In times of crisis, professional fraudsters react fast. They play on public fears, exploit overstretched systems, and take advantage of unusual times to camouflage suspicious behaviors.

80% of Certified Fraud Examiners[1] say: Fraud levels rise in times of economic distress.

But they're not the only threat to organizations working, in extremes, to protect themselves and their customers. Social and economic disruption creates new fraudsters too.

Under fresh pressure, and presented with fresh opportunities, trusted employees will also break the law—defrauding the company they work for, for example, by stealing the Personally Identifiable Information (PII) it holds.

68% of occupational fraudsters are either living beyond their means or experiencing financial difficulties.[2]

The same is true of trusted customers. In times of recession and unemployment, otherwise law-abiding citizens gain the motivation they need to commit "friendly" fraud, or make false insurance claims.

In this whitepaper, we'll examine how this wave of disruption-driven fraud can impact customer contact centers. We'll also explore how some CX leaders are taking advantage of emergent technologies such as biometrics and credibility authentication, to better protect their customers and their businesses during challenging times.

Case in point: COVID-19

400% The increase in attempted fraud cases experienced by one retail bank during the outbreak.[3]

$3.3B The value of consumer fraud losses in 2020, up from $1.8 billion in 2019.[4]

45% The increase in fraud, identity theft, and other related reports between 2019-2020, monitored by the FTC.[5]

How disruption drives contact center fraud

A sharp economic downturn, rapid shifts in living and working patterns—whatever the cause, times of disruption increase the strain on customer contact centers, and the people who work in them.

These are conditions in which fraud thrives. Already embattled contact center leaders typically find themselves facing increased fraudulent activity on three separate fronts.

The threat from career fraudsters

As evidenced by the 2020 COVID-19 pandemic, one of the hallmarks of social disruption is sudden spikes in communication between people and the organizations they depend on.

Disruption drives customers to reach out for advice and reassurance, to defer payments and sign up for emergency aid, to cancel bookings and check stock-levels. If the crisis affects the normal operation of physical branches and contact centers, the leap in the ratio of calls to available agents will be even more pronounced.

The result is an ideal environment for career fraudsters.

Cracks appear in ID and authentication processes

Faced with such overwhelming demand, it's easy for agents to put Average Handle Time (AHT) above following due process, and apply identity verification measures less rigorously and consistently than usual.

Social engineering is more likely to succeed

Service agents may be working remotely, without in-person support and training from colleagues and supervisors. At the same time, they may be striving to get to grips with new customer questions, new products, and new procedures, all occasioned by the crisis.

As a result, they are more likely to guess the correct course of action—and more susceptible to social engineering by fraudsters seeking to steal PII.

Fraudulent behavior becomes harder to spot

In turbulent times, what constitutes normal behavior changes. Legitimate customers begin to act in unusual ways, and this—combined with the overall increase in customer contacts—can create record workloads for fraud management teams. This means more fraud goes undetected, for longer.

Why fraud trends vary by industry during disruption

For a professional fraudster, their operation is a business. And like any other business leader, a period of disruption can force them to change the focus of their activities, creating different fraud trends in different industries.

For example, when disruption is accompanied by a state of social lockdown, subscription fraud against telcos becomes harder to commit—since stores are closed, and devices are harder to intercept.

Instead, agile fraudsters may switch resources to attacking banks, capitalizing on their knowledge of exactly when special relief payments will be reaching citizens' accounts.

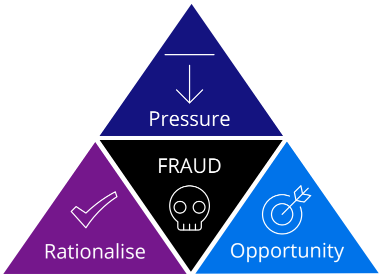
9 out of 10

anti-fraud professionals predict these will become more common in the 6-12 months following April 2020.[6]

- Charity and fundraising fraud
- Phishing through government and healthcare impersonation
- Cyberbreaches related to working from home

The threat from new fraudsters

Opportunity, pressure, rationalization. These are the three sides of the classic "fraud triangle", built on criminologist Donald Cressey's hypothesis of what a trusted employee needs to violate that trust, and commit an act of fraud.



The Fraud Triangle
During periods of social and economic disruption, both the opportunity and the financial pressure to commit fraud increases for contact center agents, and for the customers they serve.

Formerly trusted agents

For contact center agents, social disruption can lead to a dramatic change in working patterns and locations—separating them from the community of their co-workers, taking them out of sight of supervisors, and making clean-desk policies all but impossible to enforce.

At the same time, non-revenue-generating audit and compliance departments are often the first to be cut by companies facing up to hard times, weakening internal anti-fraud defenses.[7]

Just as agents find they have new opportunities to commit fraud, they—and their families—may find they have the motivation too. Any crisis that precipitates widespread job losses can place huge financial pressure on individuals and households.

Formerly trusted customers

In an era of public emergency or economic downturn, the customers talking to contact center agents will often be facing financial pressures of their own.

93% **of anti-fraud professionals** predict defrauding of government stimulus programs will increase in the 6-12 months following April 2020.[8]

86% of anti-fraud professionals predict unemployment fraud will increase in the 6-12 months following April 2020.[9]

Many will be living on a reduced income. In some scenarios, they may be struggling with unexpected healthcare costs. Much like agents, they may also find that opportunities to commit fraud are more common as governments roll out new schemes to support the worst affected. Under such circumstances, trusted customers can and do cross the line, committing fraudulent acts under their own name:

- Making false claims against insurance policies
- Applying for financial aid that they aren't entitled to
- Disputing credit card transactions after goods/services have been received

Pressure is the key driver

Studies of the Great Recession (2007-2009) suggest that pressure is the key driver of occupational fraud during challenging times.

In an ACFE survey, almost half (49.1%) of the expert respondents identified pressure as the primary factor contributing to an increase in the crime. The second most popular answer? Increased opportunity, given by 27.1%[10] of those surveyed.

One financial institution saw a

2X **increase in fraud attempts by legitimate account holders** during the COVID-19 pandemic.[11]

Using tech to fight fraud during social disruption

How can CX leaders combat the increased risk of fraud, from both career criminals and from employees and citizens driven to crime?

Just as in periods of relative stability, any comprehensive mitigation strategy should include cultural and procedural measures, as well as technological ones. For example, organizations that conduct regular catch-ups with remote-working agents—or even offer employee counselling—stand to not only strengthen their staff's resilience to social engineering, but to minimize the likelihood they will turn to crime themselves.[12]

In the remainder of this paper, however, we'll focus on our own primary area of anti-fraud expertise: the technologies that can help minimize opportunities for fraud to take place, and identify those who would perpetrate it.

Fighting career fraudsters: with biometrics

Biometric solutions are an alternative to knowledge-based authentication. Instead of an agent asking a customer for PII or a password, the customer is identified using a characteristic unique to them—for example, their voice, or the way that they type online.

As customer passwords and PII have become easier to purchase on the dark web, and organizations have strengthened their focus on customer and agent experience, biometric authentication has become increasingly popular.

In times of social disruption, however, biometrics can offer additional benefits—not least in the fight against career fraudsters seeking to exploit exceptional circumstances.

Easing the pressure on agents

When call volumes are up, and capacity is down, it's easy for agents to make mistakes. Voice biometrics free agents from the obligation to ask a series of knowledge-based authentication questions, and in doing so, help to avoid long and difficult conversations with legitimate, but equally stressed, customers.

Removing PII from agent screens

Since contact center agents no longer need to see a customer's PII to authenticate their identity, fraudsters have extremely limited opportunities to extract information for ID theft or sale.

Actively identifying known fraudsters

Just like legitimate customers, career criminals can be actively identified by their voice or their behavior. In voice applications, a biometrics solution will cross-reference a caller's voice with a database containing the voiceprints of known fraudsters.

If there's a match, the call can be flagged for further security checks, preventing successful social engineering and f fraud attempts, and minimizing the workload of fraud management teams.

"Now is the time for organizations to be bolstering their internal controls"
Bruce Dorris, President of the ACFE, in his article "Coronavirus Pandemic Is a Perfect Storm for Fraud"[13]

How HSBC UK is fighting fraud with biometrics

In a March 2020 article, Biometric Update revealed how HSBC's voice biometrics system, VoiceID, had helped protect $493M from fraudsters.

As Kerri-Anne Mills, Head of Contact Center and Customer Service at HSBC UK explained, the organization is using biometrics to both authenticate its customers and proactively identify fraudsters:

"We are now enrolling around 16,000 customers in VoiceID each week and the technology continues to be instrumental in the fight against fraud, providing a library of fraudsters' voice prints to cross check against new incoming calls."[14]

Fighting new fraudsters: with biometrics and credibility authentication

For contact center leaders working to prevent trusted employees from perpetrating fraud, introducing or expanding biometric authentication programs can be an effective strategy. But identifying customers who've been driven to break the law requires a different approach—and the emerging field of credibility authentication is working to provide it.

To understand how credibility authentication fits into fraud prevention, take the example of a customer calling their insurer's contact center.

First, the insurer's biometrics authentication system analyses the customer's voice and positively identifies their identity. Then, as the conversation continues, the insurer's credibility authentication system analyses the customer's voice as well—to confirm they're speaking as someone with a genuine insurance claim would speak, and not showing signs of trying to deceive the agent.

If the credibility authentication system does find reason to believe the customer is acting dishonestly, the claim can immediately be flagged for further investigation.

Minimizing the PII, and the opportunity

Biometric authentication minimizes the amount of PII agents need to handle to serve customers, substantially reducing their ability to sell this information, or use it to steal a customer's identity.

Identifying when customers are breaking the law

Credibility authentication helps identify when trusted customers are acting dishonestly, providing a valuable check against false claims and "friendly" fraud.

How major insurers and banks are fighting fraud with credibility authentication

Credibility authentication may be a comparatively new discipline, but it's evolving at pace. At the time of writing, multiple US and UK financial services companies are piloting credibility authentication solutions.

86% One US bank has reported accuracy rates as high as 86%.

Flexing to fight fraud with AI

Both biometric and credibility authentication systems depend on AI, rather than human resources and expertise. As a result, they can be scaled up and out quickly in time of social disruption, to help mitigate the increased incidence of attempted fraud.

First steps to combating fraud in challenging times

When our world changes, fraud thrives. For contact center and CX leaders, the best strategy is to understand how disruption drives fraud, and be prepared.

This means identifying and promoting the cultures, processes, and solutions that won't just minimize fraud during BAU, but mitigate the opportunities and pressures to commit fraud that come hand-in-hand with extraordinary circumstances.

One of the best ways to be prepared is to talk to peers in similar roles, facing similar challenges.

Simon Marchand is Nuance's Chief Fraud Prevention Officer. As well as sharing his own experience and expertise, Simon can introduce you to contact center and CX leaders at other organizations, to discuss common challenges and find new solutions. Don't hesitate to get in touch with him directly.

Simon Marchand, CFE, Adm.A. Chief Fraud Prevention Officer, Nuance Communications
Simon has over a decade's experience in fraud prevention, in banking and telecommunications. Prior to joining Nuance, he held key fraud management positions at Montreal-based Laurentian Bank, Bell Canada and was a professional inspector at Québec's order of chartered administrators.

GET STARTED
For more information go to our webpage on combating fraud in challenging times, or email us at cxexperts@nuance.com.

Endnotes
[1] https://www.acfeinsights.com/acfe-insights/coronavirus-pandemic-is-a-perfect-storm-for-fraud
[2] https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf
[3] Nuance customer
[4] https://www.ftc.gov/news-events/news/press-releases/2021/02/new-data-shows-ftc-received-22-million-fraud-reports-consumers-2020
[5] https://www.ftc.gov/system/files/documents/reports/protecting-consumers-during-covid-19-pandemic-year-review/covid_staff_report_final_419_0.pdf
[6] https://www.acfeinsights.com/acfe-insights/covidfraudsurvey
[7] https://www.acfeinsights.com/acfe-insights/coronavirus-pandemic-is-a-perfect-storm-for-fraud
[8] https://www.acfeinsights.com/acfe-insights/covidfraudsurvey
[9] https://www.acfeinsights.com/acfe-insights/covidfraudsurvey
[10] https://www.acfe.com/about-the-acfe/newsroom-for-media/press-releases/-/media/C98FABE0D12343B0AEAD528603E55772.ashx
[11] Nuance customer
[12] https://www.acfe.com/about-the-acfe/newsroom-for-media/press-releases/-/media/C98FABE0D12343B0AEAD528603E55772.ashx
[13] Coronavirus Pandemic Is a Perfect Storm for Fraud – https://www.acfeinsights.com/acfe-insights/coronavirus-pandemic-is-a-perfect-storm-for-fraud
[14] https://www.biometricupdate.com/202003/hsbc-uks-voice-biometrics-system-blocked-2x-more-fraud-attempts-in-2019

ENT_4075_01_WP, Apr 18, 2022