



POWERED BY GIANT OAK

## Solutions for Crisis-Related Fraud

### Introduction

With more than 10 percent of American workers losing their jobs in the last month, the economy is in dire straits. The US government has responded with unprecedented fiscal stimulus. But the speed and scale of the required stimulus create massive fraud risk. Key institutions like the Small Business Administration (SBA) are being asked to push out more than their annual loan portfolio in just a few weeks. In a few months those same institutions will need vastly expanded audit processes as borrowers seek the loan forgiveness promised in legislation. And governments worldwide face similar imperatives. Getting money to citizens as soon as possible while minimizing fraud is a massive challenge.

Addressing that challenge requires shifting anti-fraud practices from reactive response to proactive prevention. Government agencies and financial institutions need screening technologies that scale fast, allowing them to process most claims quickly while sending obvious risks for deeper due diligence. And because fraud is not a one-time event, these institutions' detection and response processes must incorporate low-cost continuous evaluation, both of specific entities and of random samples. Technology can help at every stage.

GOST®, by Giant Oak, is used every day by the federal government for highly-efficient screening and continuous vetting of large populations through publicly-available information (PAI). GOST® is ready now to support institutions responding to the COVID-19 crisis.

### Historical Background

Large-scale emergency spending almost always attracts fraud. By one government estimate, fully 16 percent of the \$6.3B in relief distributed to victims of hurricanes Katrina and Rita was [spent improperly](#). The COVID-19 response will be no different. In fact, it may be worse. Where disaster relief can often be spent over years, allowing agencies to build up expertise and staffing slowly, there is no time to build substantial regulatory capacity or oversight authority in today's environment.

As governments race to spend trillions of dollars of stimulus funds, one question is top of mind: how can they rapidly distribute the funds needed to relieve suffering and restore the economy while guarding against waste, fraud, corruption, and abuse?

How can institutions rapidly distribute the funds needed to relieve suffering and restore the economy while guarding against waste, fraud, corruption, and abuse?

The best case for fraud prevention in similar circumstances is the \$840 billion American Recovery and Reinvestment Act (ARRA), passed on February 7, 2009. Of the nearly 200,000 prime- and sub-contracts awarded by the ARRA, only 293 of them - or just 0.2 percent - led to “consequential investigations” of fraud according to a [government audit](#).

This should make us nervous. The majority of the ARRA funds were not spent until 2010 or 2011, allowing a full year for building due diligence and anti-fraud audit infrastructure. And while ARRA experienced little fraud, it disbursed half the funds allocated to the CARES Act in 4x the time, with 3x the budget for oversight. ARRA had roughly 12 times more oversight capacity per dollar per month. We should be worried. Spending twice as much money in a fraction of the time with 1/3 of the fraud prevention resources is a recipe for disaster.

## Stakes, Scale, and Speed

As of the writing of this paper, unemployment claims from the past month have exceeded 16 million, representing 10 percent of America’s employed population. With the COVID-19 pandemic-related social distancing requirements estimated to extend, in some form, into at least the next two months, we can expect these numbers to rise. The stakes in getting these funds out quickly is unprecedented.

The scale of the challenge is also unprecedented. In the United States alone, Congress recently passed a fourth stimulus package totaling more than \$2T. This level of stimulus is not unique to the

In the United States alone, three stimulus packages totalling nearly \$2T have been signed, with a fourth reportedly on the way.

United States. The United Kingdom (UK) has released four emergency packages, totalling aid since March 11th to £65.5B (the equivalent of ~\$81.5B). That’s almost a third more than the UK’s stimulus deployment following the 2008 crisis. Japan has approved a nearly \$1T stimulus plan. The magnitude of fraud risk across the European Union and G-30 countries is generally massive.

Speed adds another layer to the fraud challenge. COVID-19-related stimulus disbursement is intended, and needs, to be swift (data show that nearly 1/3 of Americans did not make rent last month). 125 million Americans are estimated to be eligible to receive stimulus dollars by direct deposit or mailed checks, hopefully within the upcoming weeks. Small- and medium-sized business loans have begun to be disbursed by the Small Business Administration (SBA) through a preferred bank lending network with loan limits of up to \$10M.

No agency of the federal government has spare oversight capacity at this scale. In 2019, the SBA approved 58,000 loans for \$28B. The CARES Act aims to have SBA play a role in lending more than 10 times that amount, roughly \$349B, in just the next three months. This represents a 40-fold increase in the rate of government-supported lending to small businesses.

## Early Indicators of Fraud

We are already seeing worrisome trends. As of April 9, 2020, more than 15,000 Americans had reported more than \$11,950,000 in total COVID-related consumer fraud loss, and this is before any substantial stimulus dollars have reached the pockets of individuals and businesses. This is not limited to the US. The International Criminal Police Organisation (INTERPOL) recently released a statement regarding the increase in financial crimes. The House Financial Services Committee, the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), AARP, and




others have issued similar warnings. Criminals are capitalizing on wide-spread fears to manipulate unsuspecting victims. And while we have not yet seen evidence of fraud in support to businesses, that is likely because such funds are just now beginning to flow.

The COVID-19 pandemic is not a fleeting shock. The period of acute disruption is expected to continue until a vaccine is widely available, which optimistic estimates predict for early 2021. We can anticipate that the economic disruption will last much longer than that. Scrutiny and risk-assessment for longer-term stimulus spending must continue over the course of years. If the onboarding burden is increasing by 10 times now, then investigations will need to increase comparably in four to six months from now.

### Solution: Innovate with Proactive Screening

How can we meet the dual goals of speed and fraud risk mitigation? How do financial institutions get money out fast, while responsibly completing due diligence? How do we mirror the success of the ARRA disbursement, while avoiding a Katrina-esque failure?

Technology can enable the necessary transitions from reactive response to proactive prevention. The United States has institutions that deal with fraud, but they are mostly reactive and deterrence-based. Leveraging advanced technology will get money to those who deserve it faster, while preventing criminals from exploiting this tragedy.



Leveraging advanced technology will get money to those who deserve it faster, while preventing criminals from exploiting this tragedy.

### AI, ML, and Fraud

Criminals that commit fraud come in many forms, and each one has a separate set of objectives, capabilities, and limitations. Some actors work alone, and others represent large criminal enterprises that span multiple jurisdictions. Common forms of financial fraud include synthetic identity fraud (SIF), identity theft, data breaches, and spoofing or imposter scams.

To see how advanced tools can help prevent fraud with the speed and scale necessary for the COVID-19 stimulus disbursements, we can look at the three stages of the typical fraud lifecycle: planning, launching, and cashing. In the *planning* stage criminals establish trust, which requires stealing or fabricating an identity. In the *launching* stage criminals work to fabricate histories which support their fraudulent claims. In the *cashing* stage the actual fraud is perpetrated, such as soliciting funds in the name of a false identity, or obtaining access to programs for which the criminal does not qualify (e.g. reimbursements for worker salaries to a non-existent business).



There are nuances at each level of the three steps above, but they provide a good framework for thinking about how to mitigate fraud by both individuals and representatives of larger criminal enterprises. And, because criminals are adaptive, financial institutions must deploy anti-fraud tools at each stage of the fraud lifecycle.

Currently, most anti-fraud programs are rules-based and reactive. It is easy for bad actors to adapt to rules-based systems: they just need to figure out the rules. Even if new rules were implemented, they would still be rules, and eventually illicit actors would figure them out.

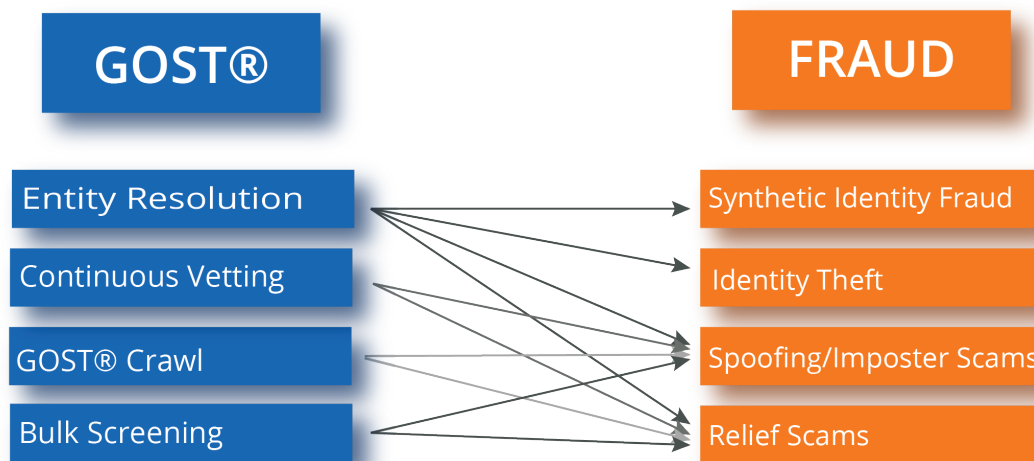
It is much harder for bad actors to adapt to fraud prevention systems driven by advanced machine learning (ML) and natural language processing (NLP) technologies. Even if they adapt to these systems at one point in time, the systems are built to learn and readjust continuously- leading to an ongoing game of tit-for-tat, which criminals cannot win for long.

Such capabilities can help disrupt the fraud lifecycle at every stage.

ML-enabled entity resolution is the key capability for disrupting fraud at the *planning* stage. At the *launching* and *cashing* stages, ML-enabled behavioral vetting using publicly-available information (PAI) is key. At *launching* criminals develop a history of behavior, a public profile, which is then exploited at *cashing*. Examining whether an applicant's claimed profile and expressed needs match their publicly observable behavior can disrupt both stages: by separating applications which should be fast-tracked because the history is consistent with the claimed need, those which display a disconnect can be forwarded for further scrutiny.

### GOST® and Fraud

GOST® (Giant Oak Search Technology) is an AI- and ML-enabled software-as-a-service (SAAS) tool that can help financial and government institutions proactively detect and prevent fraud at the scale and speed necessary for COVID-19 stimulus disbursement. GOST can be effectively deployed at every stage in the fraud lifecycle.

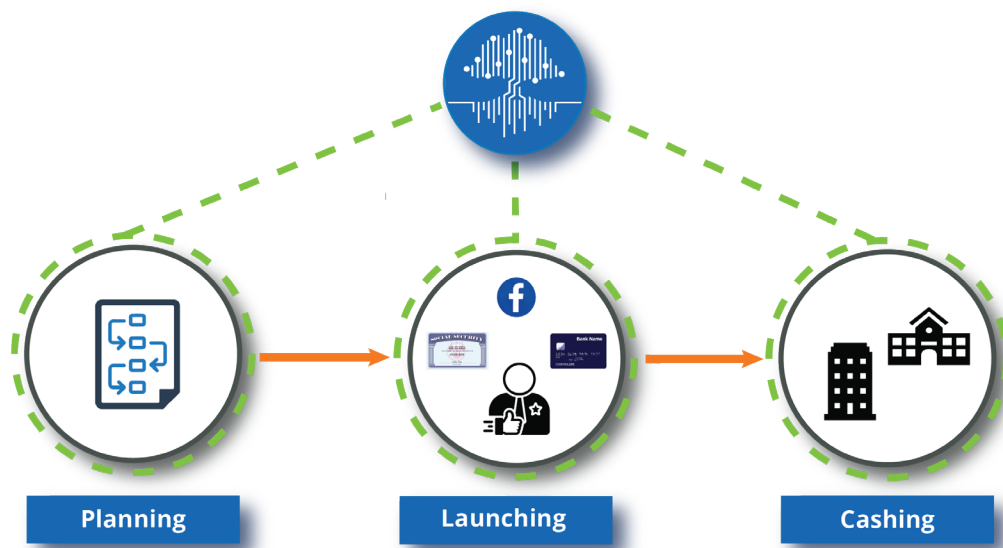


At the *planning stage*, GOST® provides ML-enabled entity resolution. By using the context surrounding an application, entity resolution algorithms can highlight when a claimed identity is associated with information that should make one think twice. A good example is a federal agency that used GOST® to confirm the identities of two individuals in Spain who had committed financial fraud through an international financial institution.

At the *launching stage* GOST® can highlight flimsy histories, allowing an institution to stop criminals before they earn an institution's trust. Overly-simplistic or unrealistically-brief histories may go undetected by extant rules-based detection systems. Tools like GOST® that leverage advanced machine-learning techniques on a wide range of PAI have a better chance of detecting thin files and past behavior that should raise concerns. For example, a federal government agency used GOST®

to reveal that an Indian industrialist living in the UK had used forged transport receipts to embezzle millions from the Reserve Bank of India. Another federal government agency using GOST® learned that a Pakistani government official had embezzled 100M RS from a provincial health department.

At the *cashing* stage GOST's continuous monitoring capability provides a way to detect erroneous patterns of behavior, enabling users to stop distributions to criminals. For longer-term fraud to be successful, an illicit actor must maintain a realistic public profile. GOST® empowers users to rapidly find information that suggests the profile a customer claims is not credible, realistic, or plausible. For example, one federal government agency used GOST® to learn that a British national who passed a superficial screening had in fact defrauded the Inland Revenue Service of £220,000 by illicitly ferrying currency from Spain. Another institution used GOST® to identify and arrest a group of criminals that were impersonating government officials in Nigeria to coax companies to give them money in the promise of receiving visas.



## Call to Action

In the coming months, governments will disburse trillions of dollars' worth of emergency relief and stimulus funding. With certainty, some small percentage of the population will try to siphon off funds for their own illicit benefit. With the unprecedented speed and scale of this stimulus, institutions need new ways to manage fraud while providing much-needed economic stability.

The solution is a transition to proactive fraud prevention practices enabled by advanced technology. Institutions can deploy GOST® at every stage of the fraud lifecycle to prevent criminals from stealing stimulus funds. Individuals and small businesses impacted by the COVID-19 crisis are depending on that money to make rent, meet payroll, and keep the economy alive. Investing in proactive screening techniques now can help agencies and financial institutions disburse funds faster and with less risk.