INVESTIGATING FRAUD IN COVID-19 GOVERNMENT PROGRAMS

How government and corporate investigators can quickly investigate the many kinds of fraud emerging from the COVID-19 pandemic and the relief programs designed to address it.

Governments around the world are spending trillions of dollars on programs to contain the COVID-19 pandemic and its economic effects. The vast sums involved and the speed at which programs are being rolled out greatly increase the potential for fraud, waste, and abuse. The agencies running these programs and the financial institutions selected to disseminate the funds are essentially forced to hand out the money now and ask questions later.

> "The vast sums involved and the speed at which programs are being rolled out greatly increase the potential for fraud, waste, and abuse."

Government and regulatory agencies worldwide have turned to Nuix software to address fraud quickly, effectively, and defensibly following financial crises, natural disasters, and other high-impact events. The US Department of Justice and most US Government inspector generals' offices use our software as the lynchpin of their investigative capabilities. This is because Nuix provides a full spectrum of tools to help you:

- Identify indicators of fraud
- Quickly preserve and process digital evidence of fraud
- Immediately make that evidence available to investigators and reviewers, even if they're working from home under social distancing or quarantine.

Using Nuix software, forensic examiners, incident responders, fraud experts, traditional investigators, grant auditors, and litigation support teams can collaborate across all phases of a fraud investigation on a single platform. You can make case data available to personnel working from home and even to partner agencies and external experts while maintaining the security and integrity of your evidence.

THE MASSIVE POTENTIAL FOR FRAUD

In March 2020, U.S. Congress passed three Coronavirus relief bills with a combined budget of more than US$2 trillion.[1] As of mid-April 2020, governments worldwide had taken fiscal actions worth around US$8 trillion including higher spending, foregone revenues and public-sector loans, equity injections, and guarantees.[2]

Governments are rolling out these programs quickly and with limited oversight with the intent to benefit the greatest number of people in the shortest possible time. Only after the money is distributed will they have the opportunity to investigate and claw back abuses—a "pay and chase" model. The fraudulent activity they'll need to investigate will take many forms:

- **Contractor fraud** such as price gouging and bidding process abuse including bribes and kickbacks
- **Healthcare fraud** including improper billing and unnecessary charges
- **Quality control** fraud due to lack of oversight, pressure to speed products to market, or intentional deceit such as supplying deficient equipment
- **Cybersecurity fraud** including trojans, coronavirus-themed phishing emails, ransomware, business email compromise, and identity theft
- **Employee misconduct** including timecard fraud, intellectual property theft, and the misuse of sensitive government or corporate data
- **Financial crimes** including money laundering and market manipulation such as pump-and-dump schemes
- **Wage replacement program fraud** such as ineligible organizations claiming the benefit; claiming for nonexistent or former staff members; or withholding "administration fees" from employee payments.

> "Only after the money is distributed will they have the opportunity to investigate and claw back abuses—a "pay and chase" model."

Examples of quality control fraud have already emerged. In one case, an entrepreneur reportedly repackaged face masks labeled "medical use prohibited" into identical packaging without the warning and tried to sell these to hospitals in Texas.[3]

The US Federal Bureau of Investigation warned of a rise in business email compromise (BEC) schemes. A BEC uses a real business email account whose credentials were stolen by a malicious actor or a fake account that appears to be from an existing supplier or a

C-level executive within the company. The scammer sends an email directing the victim to transfer funds to a trusted vendor using a different account number than usual. The targeted employee believes they are transferring the money to known vendor as in the past but the funds—often tens or hundreds of thousands of dollars—end up in an account controlled by the criminal. The FBI had seen an upsurge in BEC emails "targeting municipalities purchasing personal protective equipment or other supplies needed in the fight against COVID-19."[4]

A joint alert from the United States Department of Homeland Security Cybersecurity and Infrastructure Security Agency and the United Kingdom's National Cyber Security Centre (NCSC) warned of COVID-19-themed lures in phishing attacks and malware distribution and an upsurge in attacks against newly deployed remote access and teleworking infrastructure.[5] By mid-July 2020, the US Federal Trade Commission had received more than 68,000 COVID-19-related complaints of fraud.[6]

Wage replacement programs such as the US Paycheck Protection Program, the UK's Coronavirus Job Retention Scheme, and Australia's JobKeeper allowance have already been abused by some employers. There have been reports of employers claiming the JobKeeper allowance without meeting the eligibility requirements; pocketing the difference between the subsidy and employees' regular wages; and forcing staff members to work longer hours.[7] In the UK, HM Revenue & Customs warned of employers claiming the benefit for workers who had been furloughed (temporarily stood down) but asking those employees to keep working.[8]

THE INVESTIGATIONS BEGIN

Financial regulators are prioritizing their efforts on addressing COVID-19-related crime[9] and financial institutions are quickly adapting their anti-financial crime efforts to address regulators' concerns, identify suspicious activity, prevent crime, and identify criminals. For example, Australian bank Westpac announced it was recruiting an additional 200 people to its financial crime and compliance team.[10]

Government and law enforcement agencies have created taskforces to chase down bad actors. For example, the Coronavirus Aid, Recovery, and Economic Security (CARES) Act created the position of a Special Inspector General for Pandemic Recovery to target financial institution crime and other fraud, waste, and abuse related to coronavirus relief. This office's responsibilities are similar to the Special Inspector General for the Troubled Asset Relief Program created after the 2007–08 financial crisis.[11]

FINDING FRAUD IN A MULTITUDE OF EVIDENCE SOURCES

Using traditional digital forensic tools, investigators can only examine one data source, or one type of source, at a time. However, patterns of fraud may only become apparent after correlating many data sources including emails, documents on file shares, written correspondence, mobile devices, text messaging, cloud resources, social media, real-world activity, and patterns of behavior. Relying on human intuition to find the thread among these disparate sources is extremely challenging, particularly when time is of the essence.

Fortunately, Nuix has developed a digital investigation platform that allows law enforcement, regulatory, and corporate investigators to combine all available evidence into a single view and draw correlations across many data sources. Using Nuix's full spectrum of tools, analysts and investigators can quickly investigate all the varieties of COVID-19-related fraud we have discussed as well as those that have not yet been uncovered.

"Relying on human intuition to find the thread among these disparate sources is extremely challenging, particularly when time is of the essence."

CASE STUDY: RAPID AND ONGOING RESPONSES TO BENEFIT FRAUD

For more than six years, Nuix has worked with a federal government agency that investigates fraudulent claims to a long-running relief program. This program was set up following a global crisis under a pay-and-chase arrangement like the current COVID-19 relief efforts. As a result, it has been vital for the agency to thoroughly investigate suspect activities and hold accountable those individuals and institutions that break the law.

The agency has used Nuix Workstation to process large volumes of data—often multiple terabytes, millions of items, and dozens of source devices—quickly, reliably, and cost-effectively. It was also one of the first organizations worldwide to incorporate Nuix Investigate into its investigative workflow. With Nuix Investigate, the agency can make digital evidence accessible to around 100 field agents working across the country. This capability has proven even more critical during the current work-from-home environment.

Where investigations involve collaboration with other government agencies, this agency either transfers the data using Nuix case files or allows partner agency personnel to access its evidence directly using Nuix Investigate. This makes cross-agency collaboration much faster and less cumbersome than traditional methods.

CONTRACTOR FRAUD

To help identify price gouging and other contract violations, Nuix Workstation extracts named entities—intelligence items including people, monetary values, companies, credit card numbers, phone numbers, email addresses, web addresses, and IP addresses. For example, you could compare sums of money in post-COVID-19 contracts with prices from earlier agreements or external sources such as USASpending.gov. This would quickly reveal unreasonable price increases.

Nuix Workstation and Nuix Investigate® can also identify links between these named entities and all other indexed data including social media information. This link analysis can reveal connections between people, locations, monetary amounts, email addresses, and more to track down contractor fraud or contracting officer misconduct.

Over time, you could accumulate a data lake of historic contractor activity, charges, and actions which you could compare with current activities and behavior for suspicious changes in contrast to historic norms.

HEALTHCARE FRAUD

Using Nuix Workstation or Nuix Investigate, you can examine medical service statements for evidence of fraudulent billing. A timeline analysis will quickly reveal doctors' appointments or charges for medical services while the patient or the doctor was in quarantine or the facility was closed due to COVID-19. By analyzing the frequency of billing codes or descriptions you could quickly identify redundant, duplicate, or unnecessary medical services.

QUALITY CONTROL FRAUD

Investigative teams looking into fraudulent activity such as the supply of deficient personal protective equipment can examine communications data including email, chats, and messaging from all seized devices. You can analyze communication patterns, topics, and frequency to identify the key players, who they spoke to, and the people, sums of money, credit cards, companies, email addresses, and phone numbers they discussed. You can create custom named entities to identify names or billing codes of products, services, vaccinations, and medicine specifications to quickly find messages discussing fraud in production, quality control, testing, or delivery.

CYBERSECURITY FRAUD

Since employees working from home are tempting targets for cybercriminals, you can use Nuix Adaptive Security to identify, generate alerts on, and block the activity of malware attachments and links to malicious websites. Nuix Adaptive Security can prevent malware from executing and isolate the affected machine from the network, preventing the spread of malicious software and blocking further activity by cybercriminals seeking to compromise systems and steal valuable data.

Even while a machine is isolated from the network by Nuix Adaptive Security, security analysts can still use Nuix's suite of incident response and investigation tools—including Nuix Enterprise Collection Center, Nuix Imager, and Nuix Workstation—to collect evidence from that computer and investigate and remediate attempted data breaches.

> "You can analyze communication patterns, topics, and frequency to identify the key players, who they spoke to, and what they discussed."

EMPLOYEE MISCONDUCT

Monitoring employee activity at the endpoint can quickly identify and prevent malicious behavior such as sensitive data theft and unauthorized system access. It can help employers keep an eye on employees' activities while they're working from home and refute or substantiate allegations of employee misconduct such as timecard fraud. You can deploy Nuix Adaptive Security to remote computers and, if it identifies activity or data that warrant further investigation, initiate data collection using Nuix Enterprise Collection Center for analysis in Nuix Workstation and review in Nuix Investigate or Nuix Discover (see Figure 1 for an example of this workflow).

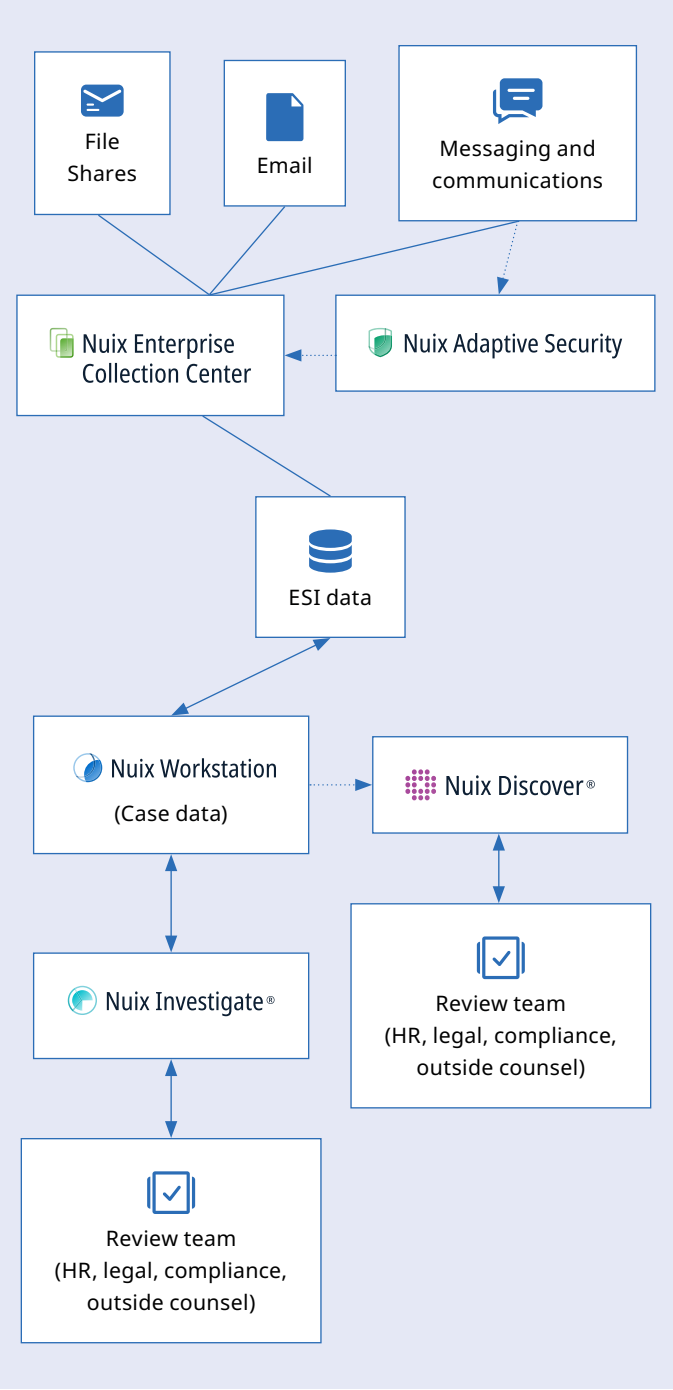

Figure 1: Investigation workflow using Nuix Adaptive Security and Nuix Enterprise Collection Center to collect data for processing, analysis, and review.

FINANCIAL CRIMES AND WAGE REPLACEMENT PROGRAM FRAUD

Financial institutions routinely use Nuix software to collect, process, investigate, and remediate money laundering and other financial frauds and scams. Taxation and welfare agencies around the world use similar workflows to investigate fraudulent claims, tax evasion, and other breaches of the law.

Using Nuix software, you can collect data from seized devices, networked sources, and cloud systems including email, storage, and social media (see Figure 2) and then apply a full suite of investigative and analytical techniques (see Analytics to the right). Processing payment data in Nuix Workstation will reveal the companies, banks, monetary values, email addresses, account numbers, and routing numbers to quickly identify improper disbursements and track those funds to be recouped.

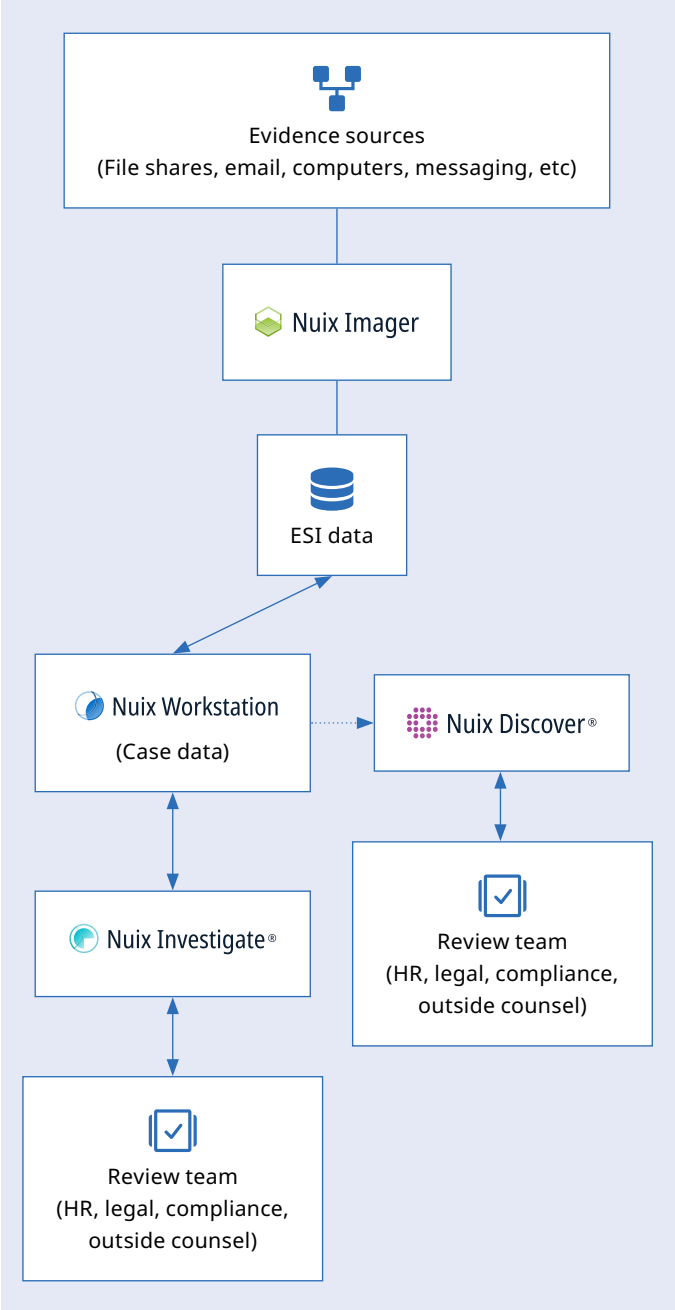

Figure 2: Investigation workflow using Nuix Imager to collect data from many enterprise and cloud sources.

ONE WINDOW INTO THE EVIDENCE

Using Nuix software, investigative teams can ingest relevant data from internal content repositories—including email systems, mobile devices, and file shares—as well as open-source intelligence from sites such as social media and forums. Our software provides a powerful arsenal of fraud investigation and analysis techniques, making it possible to spread the investigation work and assignments among team members across any number of locations.

ANALYTICS

As digital evidence becomes larger and more complex, investigators' greatest struggle is not a lack of information, but having to make sense of large datasets. Using Nuix's analytics and visualizations across large volumes of data is a fast way to locate the key facts and connections within a case. It enables investigators, even with limited technical knowledge, to follow an investigative workflow or lead down to very specific details in a matter of seconds.

> "Our software provides a powerful arsenal of fraud investigation and analysis techniques, making it possible to spread the investigation work and assignments among team members across any number of locations."

Nuix software provides a wide range of analytical techniques that can streamline investigations into COVID-19-related fraud, including:

- **Timeline**. Reviewing the content of emails, documents, phone calls, or other communications from multiple sources or custodians in the order they happened.
- **Map**. Extracting location data from digital photos, mobile devices, IP addresses, and other geotagged items, and displaying their locations and frequency on a map.
- **Date trending**. Visualizing the frequency of data over the entire case or any filtered subset, then drilling down to year, month, or day views.
- **Communication network**. Showing the interactions between persons of interest with a network diagram that shows the number of connections for each link. You can also view conversations between people that spans text messages, instant message chats, and social media messages.
- **Search and tag**. Running automated search-and-tag operations during processing, using lists of known fraud terms, to highlight potentially relevant documents at the outset of the investigation.
- **Search and filter**. Performing simple keyword searches or complex Boolean, wildcard, proximity, fuzzy, and phrase searches across all data sources at once. Investigators can filter the data by date range, file type, custodian, or any other metadata field.
- **Near duplicates**. Finding duplicate and near-duplicate text can help identify counterfeit documents and see how people shared, modified, and reused those documents over time.

- **Suspicious sums**. With sums of money from multiple sources, using techniques such as round sum or duplicate payments, Benford's law, and timeline analysis to identify anomalous figures or transactions.
- **Automated link analysis**. Automatically finding the connections within the intelligence extracted from evidence. The canvas view in Nuix Investigate shows the connections between people and the intelligence items they share to quickly identify the key players, who they were talking to, and what about.
- **Dashboards**. Building dashboards of charts and timelines to give investigators and executives strong visual indicators of trends and the progress of investigative and remediation efforts, where the numbers literally jump out at you from the sea of data.

Combining analytical techniques can help investigators progress from a bewildering volume of information to highly relevant details very quickly. For example, you could filter a large data set to display only email messages within a relevant date range that contains credit card numbers. You could then add suspect names or keyword searches to further filter the evidence. Now you can use a communication network diagram to see who is emailing credit card numbers to whom.

COLLABORATION AND REMOTE WORKING

Browser-based collaboration tools such as Nuix Investigate and Nuix Discover® make it easy for investigative teams to divide digital evidence and spread the review workload between many people. Using simple interfaces from any web browser, people with minimal training or technology expertise can search, review, tag, and analyze data.

While social distancing and quarantine measures remain in place, you can extend this collaborative model to tens or hundreds of investigators even if they're all working from home. Role-based security controls ensure you can make evidence easier to access while protecting confidential and sensitive information.

At a basic level, this is a way to share work between multiple investigators to complete the task faster. They may choose to divide the evidence by date ranges, custodians, location, language, or content. It can also be a way to distribute different types of evidence to the people most qualified to understand it and its context. Team leads can assign financial records to forensic accountants and internet activity to digital forensic specialists. In multijurisdictional investigations, investigative teams can produce evidence or intelligence packages for third parties to review, comment on, and return.

Larger law enforcement agencies have used this model to set up centralized evidence processing facilities that provide access to the results from any desktop across the organization.

"While social distancing and quarantine measures remain in place, you can extend this collaborative model to tens or hundreds of investigators even if they're all working from home."

CONTRIBUTORS

- Dan Dorchinsky, Head of Nuix US Government
- Scott Johnson, Principal Solutions Consultant
- Timothy Klinger, Head of Government Sales, Nuix Discover
- Josh Mehlman, Content Lead
- Robert O'Leary, Head of Investigations, USG & Corporate
- Paul Slater, Director Government, EMEA

SEE IT FOR YOURSELF

Get a personalized demo of our industry-leading solutions and see for yourself how our innovative software can transform data into actionable intelligence and help solve your biggest fraud investigation challenges.

www.nuix.com/cov-demo

REFERENCES

1. *H.R. 6074: Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020*, *H.R. 6201: Families First Coronavirus Response Act*, and *H.R. 748: Coronavirus Aid, Relief, and Economic Security Act*
2. *Vitor Gaspar, W. Raphael Lam, and Mehdi Raissi, Fiscal Policies to Contain the Damage from COVID-19, International Monetary Fund, April 15, 2020*
3. *J. David McSwane, He Removed Labels That Said "Medical Use Prohibited," Then Tried to Sell Thousands of Masks to Officials Who Distribute to Hospitals, ProPublica, June 25, 2020*
4. *Federal Bureau of Investigation, FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic, April 6, 2020*
5. *US Department of Homeland Security, Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors, April 8,2020*
6. *US Federal Trade Commission, FTC COVID-19 and Stimulus Reports, July 14, 2020*
7. *Caitlin Fitzsimmons, Tip-offs point to employers cheating staff on JobKeeper, Sydney Morning Herald, June 14, 2020*
8. *Chris Giles, HMRC chief warns job retention scheme a target for organised crime, Financial Times, April 9, 2020*
9. *Australian Securities and Investments Commission, 20-086MR Details of changes to ASIC regulatory work and priorities in light of COVID-19, April 14, 2020*
10. *Aimee Chanthadavong, NAB to take AU$1.14 billion hit to its first-half net profit, ZDNet, April 20, 2020*
11. *Ben Wilhelm, Special Inspector General for Pandemic Recovery: Responsibilities, Authority, and Appointment, Congressional Research Service, April 13, 2020*