


TIP SHEET

Vetting businesses: six tips to protect your agency—and the public—from fraud in today's digital environment



Safeguard your business creation process and the data your jurisdiction needs to make critical decisions.

The official creation of a business starts with government agencies like the Internal Revenue Service, Secretary of State and State Tax Authorities. Even in normal times, criminals need the approval of these agencies to establish fraudulent businesses to launder money, avoid taxes, conduct fraud or send money overseas. In the present environment, the risk is even greater. Oversight experts and veteran watchdogs warn that business-focused stimulus funds are highly vulnerable to fraud and abuse.¹

Large, sophisticated fraud networks based overseas are working hard to get their hands on American's hard-earned taxpayer dollars. The FBI cautions that hackers and scammers are quick to use new crises to ramp up online attacks.² History has shown that criminals take every opportunity to perpetrate fraud when unusual circumstances result in less upfront oversight.

Part of the responsibility for ensuring that financial aid only goes to legitimate U.S. businesses and citizens lies with government agencies. As the authority on companies in their jurisdiction, government agencies must be vigilant in preventing fraud when a business is initially created and throughout the lifecycle of that businesses' account.

Government agencies want to get businesses working and benefits into the hands of people and businesses who need it quickly. But fraud flourishes when oversight is deficient. You can look at recent history—the Hurricane Katrina disaster relief in 2005, the big bank bailout of 2008—to see how criminals moved in quickly to fraudulently acquire millions of U.S. dollars, capitalizing on the abundance of available money and lack of controls.

All new crises create similar vulnerabilities. If government agencies have challenges properly authenticating business applicants on the front end, much of the money intended to keep businesses afloat could be stolen by fraudsters.

Here are six strategies to help protect your agency from fraud intended to target the Small Business Administration (SBA) stimulus funds:

1. Check digital identities and documentation

With “stay-at-home” orders in place, or in the process of loosening, widespread fear of infection when going out in public may persist. Most business owners will register their business and apply for stimulus loans online.

Frequent data breaches mean stolen identity data is readily available on the Dark Web, giving fraudsters the information they need to impersonate legitimate citizens. Cybercriminals are sophisticated in their use of bots and synthetic identities to create fraudulent businesses.

It's up to government agencies to be vigilant in proactively checking digital identities by using tools that utilize global shared intelligence to assess IP address risk and recognize device location; and that understand the behavior and personas of known threats so that you can begin the process of confirming that applicants are who they claim to be.



Government agencies must be empowered with the right solutions to properly authenticate business applicants on the front end in order to prevent fraudsters, both domestic and foreign, from receiving funds intended to keep U.S. businesses afloat.

2. Use authentication solutions that work across multiple device types

Businesses have access to your agency from multiple channels. They can use their laptop computer, tablet or smartphone to transact with your agency. Your agency must be able to associate individual identities with their various digital devices and answer questions such as:

- Was this device previously used for fraudulent activity anywhere in the world?
- Is this device connecting from a foreign country?
- Was this particular risky device used to create multiple applications?

Identity tools that utilize global shared intelligence platforms to authenticate business applicants in near real-time are a critical layer in your front-end vetting process.

3. Conduct due diligence of officers and responsible parties

To verify businesses, your agency must also authenticate the person registering the business and the owners/authorized representatives of that business. You need answers to questions such as:

- Is the person registering the business who they claim to be?
- Is the person truly associated with the business as they say they are?
- Could the officers' identities be synthetic, stolen or manipulated?
- Are the officers alive or dead?
- Are the officers related or connected to any known bad actors?

Confirming that the person registering the business and its' officers are legitimate and not associated with prior fraud or crime is a critical piece of the due diligence process.

4. Vet businesses up front

Before approving the registration of new businesses, particularly those businesses likely to conduct suspicious activities, government agencies must be able to answer questions such as:

- Is this a legitimate U.S. business?
- Is the business or officers on any U.S. or foreign watch lists or sanction lists?
- How long has this company been in business?

Vetting of the business and the individual registering the business should be done on the front end. Attempting to claw back money later is likely to be impossible, especially if the fraud has been perpetrated by foreign fraud rings.

Mistakes can snowball into additional fraud if a fake business is approved and synthetic employees then apply for fraudulent unemployment benefits, tax refunds, etc. Issuing money to fraudulent businesses keeps U.S. dollars from going to legitimate U.S. businesses and their hard-working employees in a time of need.



5. Protect your data

Decisions your agency makes today about a business can have repercussions for years. If you don't have processes in place to prevent fraudsters from creating fake businesses and conducting suspicious activities, they'll get into your system. Once registered in the system, they can access your agency's services, conduct fraudulent transactions and potentially apply for more financial assistance in the future.

Preventing the creation of fraudulent businesses in the first place eliminates many headaches and losses down the road. Keep your data clean by locking fraudsters out now.

6. Be ready to defend against emerging fraud threats

Fraud prevention measures that worked last year or even last month may not be effective today. Criminals are continually refining their techniques and searching for new vulnerabilities. If your controls aren't evolving along with the ever-changing fraud landscape, you may have a false sense of security.

The best fraud solutions include artificial intelligence and machine learning that enable them to rapidly adapt to new fraud trends. Now is the time to evaluate your capabilities and tighten controls.

Your agency needs the ability to detect and block fraud. Even a small percentage of funds going to fraudsters could mean a loss of millions of U.S. dollars, with little chance to recoup those stolen monies. The media, watchdog groups and your citizens will demand accountability. To minimize fraud losses and mitigate reputational risk, oversight must be implemented when businesses are created, long before the money begins to flow.

The right risk management solutions can facilitate better, faster, real-time decisioning so fraud prevention is effective and legitimate businesses don't face unnecessary friction when applying for aid. Your government agency has an obligation to help ensure that much-needed economic relief goes to qualified recipients. That responsibility can only be properly managed if you have the solutions in place to authenticate new businesses before they are registered and to conduct ongoing monitoring of existing businesses for the lifecycle of their account.

For more tips on vetting businesses in times of increased fraud, please contact your LexisNexis Risk Solutions representative or call us at 888.579.7638.



Government

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our government solutions assist law enforcement and government agencies with deriving insight from complex data sets, improving operational efficiencies, making timely and informed decisions to enhance investigations, increasing program integrity and discovering and recovering revenue.

¹ <https://abcnews.go.com/Politics/experts-warn-big-dollar-fraud-22-trillion-coronavirus/story?id=69966232>

² <https://www.cnet.com/news/fbi-issues-warning-for-covid-19-stimulus-package-scams/>