A GUIDE TO

Using Analytics to Control PPP Loan Risks

Introduction

In March 2020, social distancing steps forced millions of small businesses to close or operate at minimum capacity. The unemployment rate spiked and many workers were left without paychecks. Congress created the Paycheck Protection Program (PPP) as part of the *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act) to help alleviate the negative impact of the COVID-19 pandemic.

Any disaster can make organizations vulnerable to large-scale fraud and scams, and COVID-19 is no exception. Financial institutions at the center of the storm face tremendous risks and challenges in the PPP loan and forgiveness process. This article explores these risks, provides insights on red flags, and suggests tangible analytical approaches to help banks to prepare for and mitigate risks by using unsupervised machine learning (UML) techniques to monitor customers' changes in behavior.

Banks, PPP Lending, and Risks

On top of the economic hits they are experiencing because of COVID-19, banks also face risks on many fronts, including:

Fraud Risks

Early signs are **already emerging**, and it is estimated that the first-party fraud rate could be about 10 to 12% for PPP loans. Third-party fraud through identity theft targeting banks with weak risk management frameworks could be on an even larger scale. In addition, when a bank employee is involved, the liability of misconduct on the part of the bank is almost unquestionable.

Operational Risks

Banks might encounter efficiency issues while trying to issue loans or process forgiveness requests because of practical challenges related to **updated forms**, **the E-Tran system**, **overwhelmed call centers**, and other **operational challenges**.

Compliance Risks

Because of the sheer volume and speed of the PPP program, existing vulnerabilities within a bank's compliance programs could be exposed, and with the heightened operational and fraud risks mentioned above, existing gaps might also be amplified.

Reputational Risks

In addition to accusations of **unfair treatment** and inefficiency, banks could face reputational damage when denial of PPP loans or issues in processing forgiveness requests result in negative media attention.

Bad Debt Risks

Banks might have a significant remaining balance of PPP loans that were not forgiven due to various reasons and that might be at higher risk for future default.

Above all, fraud and operational risks are especially high during the PPP process. If banks can control fraud risks and reduce operational risks, other risks will also be mitigated.

PPP-Related Fraud Risks

The best way to achieve risk mitigation is to create evidence-driven, repeatable, and consistent analytics to help identify fraud red flags and to provide data points to enable streamlining, streamlining which will increase operational efficiency and reduce operational risks.

- **Provide data points as key references to automate controls.**

In order to process the loans and associated forgiveness requests expeditiously, banks need to streamline processes but continue to conduct adequate due diligence to address the risks highlighted above. The main requirement here is using referential data points that are evidence-driven. Profiling existing customers using February 15th and state-specific lockdown dates can provide vital points for banks to make quick decisions and build or improve processes around them. Examples are provided in the following section to illustrate the application of an unsupervised machine learning (UML) segmentation technique and scoring technique.

- **Profile data to mitigate risk application and forgiveness fraud.**

Profile data to mitigate risk application and forgiveness fraud. Transactional profiling can help to develop scorecards to risk-rank applications and requests when combined with red flag indicators. We provide one example in using UML techniques to build indicators through correlation of date-based activity variations versus KYC data.

- **Provide documentation.**

A consistent analytical approach, evidence-based decision-making, and risk mitigation can be instrumental for banks to avoid compliance disasters. Analytical context helps demonstrate that due diligence is being applied, and it creates a clear trail of documentation to prove sound compliance framework and operational practice.

To further explain how to apply analytical context, we first summarize a list of specific PPP-related red flags in Exhibit 1. We then provide detailed examples on how to build analytics around them. From the time-of-happening perspective, PPP-related fraud can hit during the application stage as well as the forgiveness stage. The following three broad categories are our starting point to map PPP-related fraud red flags:

- First-party fraud, when customers themselves are trying to defraud the bank
- Third-party fraud, when fraudsters use false identities and submit applications using stolen identification or synthetic identities
- General transactional fraud or general benefit fraud, which occurs during a disaster relief funding situation such as with **Federal Emergency Management Agency funds**.

EXHIBIT 1: PPP-RELATED RED FLAGS

Red flags	Description	Application stage	Forgiveness stage
Inaccurate payroll	Borrowers inflate payroll to qualify for a higher loan amount.	✓	
Ineligible size	A business has more than 500 employees but still applies.	✓	
Not in business	Borrowers were not open or not in business before or at the time of COVID-19 impact. (The requirements are that the business must have been in operation on Feb. 15, 2020, and have either had employees for whom the small business paid salaries and payroll taxes or paid independent contractors as reported on a Form 1099-MISC).*	✓	
Lack of key documentation or forgiveness evidence	Borrowers cannot provide key documents, or they try to use alternatives, including tax documents and minimum required beneficiary ownership (BO) information.	✓	✓
Identity theft or mismatched names	▸ Fraudsters steal identities of owners of small businesses that are not eligible** (often friends or relatives of business owners) and file false applications. ▸ Funds are dispersed to an account that has a name different from that of the applicant.	✓	✓
Complex beneficiary ownership	A minimum set of information needs to be collected for BOs with more than 20% of the ownership, including owner name, title, ownership %, taxpayer identification number, address, and date of birth; such information could be distorted or omitted so that multiple applications could be filed at different institutions (loan stacking).	✓	
Error in forgiveness calculation	Borrowers try to manipulate funds ratio to meet forgiveness requirements.		✓
Suspicious information updates	Data points, such as address, name, or phone number, change from those used during the application.		✓
Compliance red flags	General compliance red flags, such as adverse media hits, sanctions hits, and anti-money laundering (AML) alerts, emerge.	✓	✓
Illicit funds claimed as COVID-19 relief loan	Money launderers could take over a stressed small business and use the account to launder dirty money by claiming illicit funds as relief loans. Although this is technically an AML red flag, it could be detected by fraud analytics.	✓	✓
Coordinated fraud red flags	Organized crime rings submit multiple applications using identities phished or stolen from eligible businesses. The applications are likely to contain valid identities, but they might also have suspicious correlations (such as in the receiving account numbers or digital contact information) that indicate coordinated fraudulent activities.	✓	

* "Business Loan Program Temporary Changes; Paycheck Protection Program,"

** Ibid

Applying Analytical Context to Monitor Red Flags

Using advanced UML to monitor changes in behavior can provide analytical context to detect fraud red flags. We discuss here three examples in detail.

Example 1: Not-in-business red flag

Because most PPP borrowers are already banks' customers, banks have a certain level of transactional data that can be used to build behavioral profiles. Analytics such as time series analysis can be explored to monitor changes in borrower behavior over time. Cases in which the borrower was not in business prior to the PPP designated date (Feb. 15, 2020) or do not have transactions prior to that date would be a clear red flag.

Although many businesses are affected by COVID-19, there are some businesses that are not, such as online education, remote working assistants, and others. To distinguish whether a business is negative or positively affected by COVID-19, change point detection or forecasting methods help to identify the time-of-change (if any) as well as the direction (increasing or decreasing) and magnitude of change. This information can be used to flag the lack of variation in transactional time series, indicating higher risk that the borrower was not previously in business or was not operating on the designated date. The analysis results also provide data points on the extent to which the borrower was affected financially.

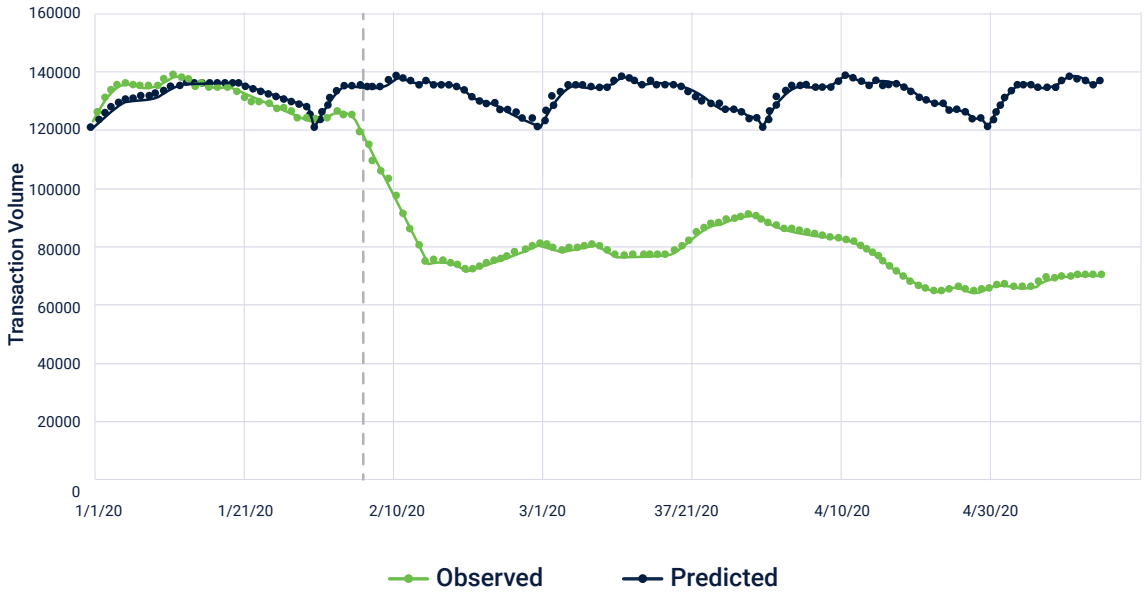

Figure 1: Using time series analysis to predict transaction volume and identify change points.

Source: DataVisor

Example 2: Inaccurate payroll and ineligible size red flags

Misreported information, such as inflated payroll or ineligible company size, can be identified by comparing known businesses with a profile similar to that of the borrower. Banks can segment known businesses according to industry or location and create clusters based on payroll data and employee size within each segment. A borrower's claimed payroll and employee size are compared with peers in its corresponding segment(s) to provide an indication of risks.

Multiple segments can be established to analyze the data from different aspects. For example, creating one set of clusters based on the industry type, a set based on business location, a set based on the combination of industry type and location, and another based on the combination of industry type, location, and revenue can reveal valuable insights. This analysis provides a fine-grained view of the financial activities of known businesses, which also allows a new borrower's information to be analyzed from multiple dimensions.

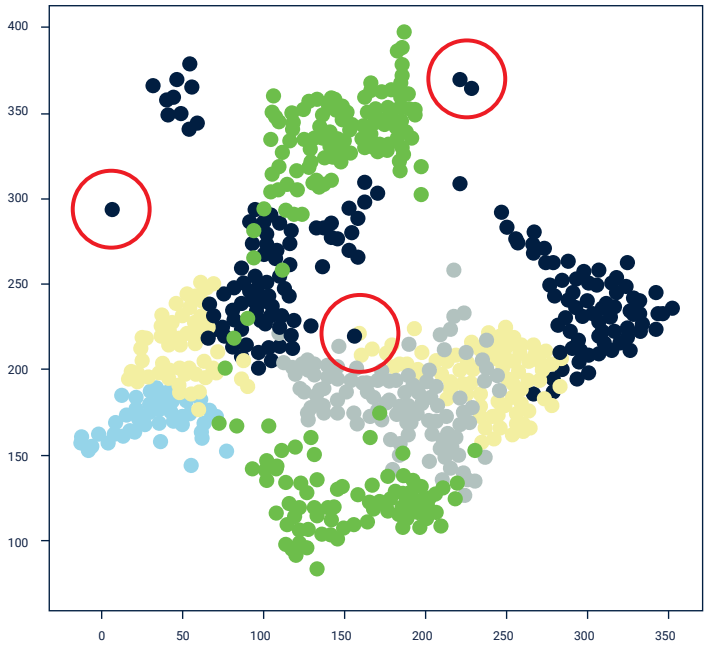

Figure 2: Example of using clustering to identify red flags. The colors correspond to the industry of the businesses, the X axis is company size, and the Y axis is payroll size. Businesses in the same industry tend to cluster together. Those that are not like others in their peer group can be identified as outliers (red circles).
Source: DataVisor

Banks can design scorecards to help streamline applications, which helps with documentation.

A consistent analytical approach, evidence-based decision-making, and risk mitigation can be instrumental for banks to streamline processes and improve documentation.

Example 3: Correlated fraudulent applications

In response to government financial incentives such as PPP, there has been a surge in email phishing campaigns targeting businesses with the goal of harvesting sensitive information. These stolen identities are subsequently used to submit fake loans, often perpetrated by organized crime. In this case, the loan applications are likely to contain valid information and might not trigger red flags. Yet the manner in which these fraudulent activities are conducted can result in correlations between the applications that are detectable. For example, the funds might be designated for the same receiving account number (or bank), or the provided email contacts might be newly registered or from a custom domain intentionally made to look similar to the actual business domain.

Instead of reviewing each application individually, banks can explore new processes that effectively monitor multiple correlated applications together. In addition to increasing efficiency, this approach can help identify suspicious relationships among borrowers that might be indicative of coordinated fraudulent activities.

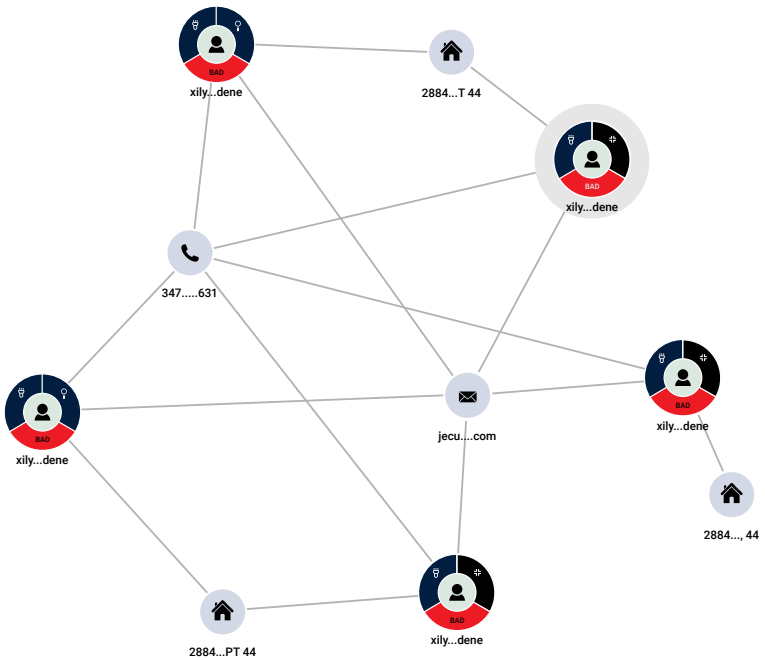

Figure 3: Correlated fraudulent applications
Source: DataVisor

Combating Financial Crimes

Banks face tremendous challenges while coping with new regulations and events such as the PPP program, particularly in anticipating potential risks and preventing fraud. Analytical context combined with unsupervised techniques enable the identification of new trends and facilitate a deeper understanding of information in the collected data. By identifying patterns and correlations, these technologies can be an effective approach for banks to mitigate risk and combat financial crimes.

LEARN MORE

Haibo Zhang
Managing Director, Crowe
+44 (0) 736 829 0772
haibo.zhang@crowe.com

Ting-Fang Yen
Director of Research,
DataVisor Inc.
tingfang.yen@datavisor.com

Tom Shell
Head of Partnerships and Alliances,
DataVisor Inc.
+1 734 619 0469
tom.shell@datavisor.com

About DataVisor

DataVisor is the leading fraud detection platform powered by transformational AI technology. Using proprietary unsupervised machine learning algorithms, DataVisor restores trust in digital commerce by enabling organizations to proactively detect and act on fast-evolving fraud patterns and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of more than 4B global user accounts, DataVisor protects against financial and reputational damage across a variety of industries, including financial services, marketplaces, ecommerce, and social platforms. DataVisor was recently recognized by Gartner as a Cool Vendor in the Identity and Access Management and Fraud Detection report and is a recipient of multiple industry awards.

About Crowe

Crowe LLP is a public accounting, consulting and technology firm with offices around the world. Crowe uses its deep industry expertise to provide audit services to public and private entities. The firm and its subsidiaries also help clients make smart decisions that lead to lasting value with its tax, advisory and consulting services. Crowe is recognized by many organizations as one of the best places to work in the U.S. As an independent member of Crowe Global, one of the largest global accounting networks in the world, Crowe serves clients worldwide. The network consists of more than 200 independent accounting and advisory services firms in more than 130 countries around the world. and Fraud Detection report and is a recipient of multiple industry awards.