Benchmarking Fraud Detectors on Private Graph Data

Alexander Goldberg
Carnegie Mellon University
Pittsburgh, PA, USA
akgoldbe@andrew.cmu.edu

Giulia Fanti
Carnegie Mellon University
Pittsburgh, PA, USA
gfanti@andrew.cmu.edu

Nihar Shah
Carnegie Mellon University
Pittsburgh, PA, USA
nihars@andrew.cmu.edu

Steven Wu
Carnegie Mellon University
Pittsburgh, PA, USA
zhiweiw@andrew.cmu.edu

Abstract

We introduce the novel problem of benchmarking fraud detectors on private graph-structured data. Currently, many types of fraud are managed in part by automated detection algorithms that operate over graphs. We consider the scenario where a data holder wishes to outsource development of fraud detectors to third parties (e.g., vendors or researchers). The third parties submit their fraud detectors to the data holder, who evaluates these algorithms on a private dataset and then publicly communicates the results. We propose a realistic privacy attack on this system that allows an adversary to de-anonymize individuals' data based only on the evaluation results. In simulations of a privacy-sensitive benchmark for facial recognition algorithms by the National Institute of Standards and Technology (NIST), our attack achieves near perfect accuracy in identifying whether individuals' data is present in a private dataset, with a True Positive Rate of 0.98 at a False Positive Rate of 0.00. We then study how to benchmark algorithms while satisfying a formal *differential privacy (DP)* guarantee. We empirically evaluate two classes of solutions: subsample-and-aggregate and DP synthetic graph data. We demonstrate through extensive experiments that current approaches fail to provide utility when guaranteeing DP. Our results indicate that the error arising from DP trades off between bias from distorting graph structure and variance from adding random noise. Current methods lie on different points along this bias-variance trade-off, but more complex methods tend to require high-variance noise addition, undermining utility.

CCS Concepts

• **Security and privacy**; • **Computing methodologies** → *Cross-validation*; • **Applied computing** → Electronic commerce;

Keywords

fraud detection, differential privacy, graph data, model evaluation, synthetic data

Conference'17, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

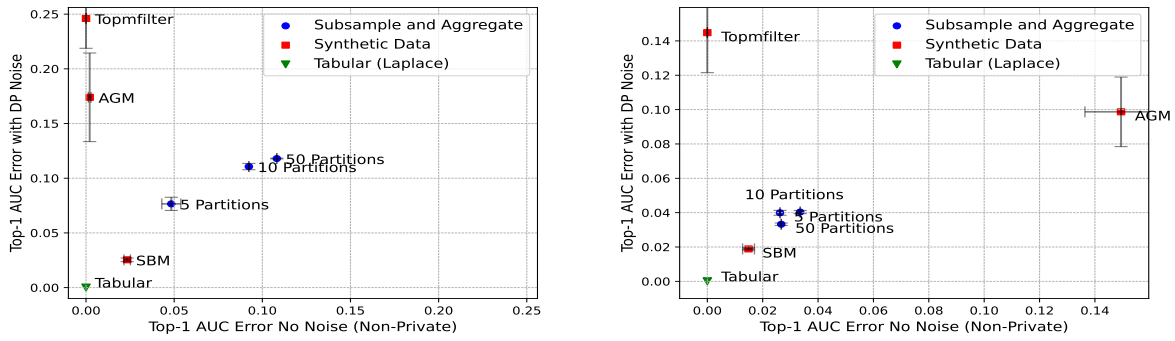
ACM Reference Format:
Alexander Goldberg, Giulia Fanti, Nihar Shah, and Steven Wu. 2025. Benchmarking Fraud Detectors on Private Graph Data. In . ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Fraud constitutes a pernicious problem across numerous domains, manifesting as fake product reviews, fraudulent payments, and the resale of stolen goods, among other harms [6]. The scale of fraud losses is driven in part by the difficulty of detecting fraud: today, the problem is primarily handled by automated detectors with high false positive and false negative rates. Although many organizations dedicate entire teams to fraud detection, other organizations outsource the development of fraud detection mechanisms to third parties, such as vendors of fraud detection software and/or third-party researchers [7, 26, 39]. However, effective outsourcing requires enterprises to share internal fraud data, which can be challenging due to privacy regulations (e.g., GDPR) and/or the risk of leaking trade secrets through shared datasets. As a result, the lack of publicly shareable data has limited research progress on detection of fraudulent behaviors in privacy-sensitive domains. For example, in scientific peer review, there is a lack of data on reviewer-paper assignments. This limits researchers' ability to evaluate solutions to the problem of detecting rings of colluding reviewers [29, 42].

Problem Statement. In this work, we explore a paradigm for outsourcing fraud detection in which data does not leave an organization's boundaries. Instead, third-parties submit fraud detection algorithms based on existing techniques—including domain knowledge and public data—which are evaluated and ranked by the data holder. These third parties may be motivated by financial/reputational rewards for the winning developers, based on a leaderboard [20]. We study this setting under two key constraints that have not been explored together previously:

(1) *Private algorithm evaluation*: We observe that if the accuracy of a fraud detector is released directly, it can leak sensitive information about the underlying test data (Section 2). We therefore consider methods for evaluating algorithms, and releasing their results, under a differential privacy (DP) constraint [10].
(2) *Graph-structured data*: Many prominent fraud domains, such as financial fraud or product review fraud, have graph-structured datasets. We focus on fraud detection algorithms (and privacy solutions) that can be applied to graph-structured data.



(a) Amazon **(b) Yelp**

Figure 1: Comparison of DP benchmarking methods for releasing the best AUC score among 10 fraud detectors with privacy budget of $\varepsilon = 5.0$. The horizontal axis captures error due to inductive bias (i.e., the underlying graph model, without DP noise); the vertical axis captures error including DP noise. More complex synthetic data methods (Topmfilter and AGM) can model the data without privacy, but suffer from high variance due to DP noise addition, undermining utility. Subsample-and-aggregate distorts graph structure extensively, even before adding random noise to outputs. All current methods incur large utility cost on graph data compared to tabular data. Error bars show the standard error of the mean across 10 simulations of each method.

More precisely, we consider a *benchmarking server*, which has a private graph G consisting of a set of known fraudulent vertices V_1 (of size n_1) and a set of benign vertices V_0 (of size n_0).

The benchmarking server's goal is to *evaluate* one or more fraud detection algorithms and *communicate* the result back to the algorithm designers. The benchmarking server receives a fraud detection algorithm $\mathcal{A}$. The fraud detection algorithm takes as input a vertex v and the entire graph G and outputs $\mathcal{A}(G, v)$ which is a numerical score where a higher score indicates a higher likelihood of fraud. For example, the fraud detection algorithm could score a vertex by its degree. The benchmarking server returns an *accuracy statistic* for the fraud detection algorithm on graph G. Concretely, we consider the *AUC score*, which is defined as:

$$f_{\text{AUC}}(\mathcal{A}, G) = \frac{1}{n_1 n_0} \sum_{v_0 \in V_0} \sum_{v_1 \in V_1} \mathbb{1}[\mathcal{A}(G, v_1) > \mathcal{A}(G, v_0)].$$

The AUC score represents the probability that a randomly chosen fraudulent vertex is scored higher than a randomly chosen benign vertex. It is a commonly used accuracy statistic for class-imbalanced binary classification problems like fraud detection [13].

Challenges and Approach. Existing techniques for differentially private release of statistics cannot be easily applied to graph-structured data (Section 3.2). The main challenge is that benchmarking fraud detection algorithms on graph-structured data relies on high-sensitivity queries over the graph, meaning that the query result can change significantly if even a single node's neighbors are altered in the graph (Definition 3.2). Making such algorithms DP requires large amounts of noise, undermining utility.

The goal of this work is to instantiate and benchmark different classes of techniques for evaluating fraud detection algorithms over graph-structured data under a DP constraint. We evaluate two approaches for dealing with high-sensitivity queries: *(1) Subsample-and-aggregate* partitions the dataset into non-overlapping datasets, then evaluates the fraud detectors over each partition. The average accuracy over the partitions is low-sensitivity, and can be released with less noise than without partitioning. *(2) Synthetic graph data* generates a DP copy of the true graph; then, fraud detectors are evaluated on this synthetic graph.

Contributions. Our primary contributions are:

(1) We formulate the problem of *differentially private benchmarking of fraud detectors on private graph data.* **We describe a simple privacy attack on a system that benchmarks user-submitted algorithms on private data. In simulations of a deployed facial recognition benchmarking system, we show that this attack is practical**—concretely, our attack achieves near perfect accuracy in identifying whether individuals' data is present in a private dataset, with a True Positive Rate of 0.98 at a False Positive Rate of 0.00.

(2) We then evaluate the potential of differential privacy as a solution concept for preserving privacy of graph data used in a benchmarking system. Across methods, **we observe a severe trade-off between bias introduced by distorting the graph and noise required to compensate for computing high sensitivity statistics on the graph.** This result is captured in Figure 1, which shows the error in privately benchmarking the best AUC score among a set of 10 fraud detectors. We plot the error of each DP benchmarking method without noise added (inductive bias) against error after adding noise to ensure differential privacy. Among synthetic data methods, more complex methods (TopmFilter and AGM) have lower inductive bias, but much higher noise addition to preserve privacy than the simpler SBM. Subsample-and-aggregate tends to distort graph structure extensively, even before adding random noise to outputs, but then has low additional error from the random noise. All current methods to satisfy DP on graph data incur large utility cost compared to tabular data.

(3) To explain these results, we conduct detailed ablations on both subsample-and aggregate and synthetic data methods. While these methods introduce inductive bias in different ways, they exhibit a similar trade-off — the less we bias our graph representation, the more noise we must add to satisfy DP.

Our code is available at `https://github.com/akgoldberg/private_fraud_benchmarking`.

2 Privacy Risk

We start by describing an attack that a malicious actor can use to compromise the privacy of an individual included in the graph dataset used for algorithmic benchmarking.

2.1 Privacy Attack

Consider a bad actor who wishes to answer a binary query, such as whether an edge exists between two vertices in the graph. The adversary needs three capabilities. (1) *An accurate fraud detector:* for example, a known algorithm from the literature which does better than random (AUC > 0.5). (2) *An inaccurate fraud detector:* for example, scoring vertices at random (expected AUC $= 0.5$). (3) *The ability to identify vertices in G:* this depends on what information the private server gives to the fraud detection algorithm.[1] In many cases, G may include extensive metadata per vertex, which makes it easy to identify vertices. Even without metadata, there are many de-anonymization attacks leveraging only the graph structure (see [18] for a survey), which enable an adversary to identify vertices.

Algorithm 1 Attacker's Submission to the Benchmarking Server

Require: Accurate fraud detector $\mathcal{A}$, pair of vertices v_1, v_2.

1: Check if an edge exists between v_1 and v_2 in private graph G.
2: **if** edge (v_1, v_2) exists **then**
3: Run accurate fraud detection algorithm $\mathcal{A}$ on G.
4: **else**
5: Return a random fraud label for each vertex in G.
6: **end if**

The adversary submits a "fraud detector" to the benchmark described in Algorithm 1. The adversary identifies the relevant pair of vertices, and runs the accurate fraud detector if an edge exists between the vertices or an inaccurate fraud detector otherwise. If the adversary observes a high AUC score, they learn that an edge exists, while if they observe a low AUC score they learn that the edge does not exist. In effect, the benchmark allows a malicious actor to answer any binary query on G by encoding the query as either a high-accuracy or low-accuracy fraud detector. The privacy attack we describe above applies to a range of benchmarking systems that evaluate user-submitted algorithms on private data, as demonstrated in the next section.

2.2 Attacking a Real-World Benchmark

To demonstrate the practical implications of the attack, we take an existing privacy-sensitive application as a case study: the National Institute of Standards and Technology (NIST) Face Recognition Technology Evaluation (FRTE). The FRTE benchmarks algorithms for facial recognition on sensitive private datasets of face images like mugshots, visa applicants, and border-crossing photos. The FRTE benchmarks the task of "1:N face identification". A 1:N face identification algorithm matches a given "probe image" against a large "gallery dataset" of images, returning an image in the gallery of the same person. While the dataset consists of face images, not a graph, the same attack proposed for graph data can be applied to the face recognition benchmark system.

Specifically, an attacker with access to a reasonably accurate facial recognition algorithm can exploit the benchmarking system to determine whether one or more specific individuals' faces are included in the gallery dataset; for example, suppose that an attacker wants to know if Bob is in the gallery dataset. The attacker obtains an image of Bob. When the attacker's submission searches the gallery dataset for a given probe image, the attacker first uses the accurate facial recognition algorithm to check if Bob's image matches any image in the gallery dataset. If yes, they use the accurate algorithm on the *actual probe image* (i.e., not Bob). If Bob is not in the gallery, they use the inaccurate algorithm on the probe image. A high accuracy score on the benchmark implies Bob's presence, while a low score indicates his absence.[2]

2.3 Effectiveness of the Attack

To evaluate the practical viability of the attack, we simulate the 1:N face recognition benchmark using the publicly available CelebA dataset, which contains faces of over 10,0000 celebrities [31]. We use an open-source, deep learning-based facial recognition model ArcFace [8] as the accurate model. The attacker uses the face recognition model to generate embeddings (templates) of images and then performs "identification" using cosine similarity between embeddings. We vary the adversary's capabilities by reducing the dimension of the embeddings used by the model from 512 to 64 and 32. Then, true positive and false positive rates of the attack can be computed by varying the threshold at which the attack concludes that an attack image is present in the private data. In Figure 2, we show the ROC curve of the attack. **Using 512-dimensional embeddings, the attack achieves a TPR of** 0.98 **at an FPR of** 0.00**, successfully identifying 98 out of 100 gallery members while avoiding false matches.** Even with 64- or 32-dimensional embeddings, the attack remains effective, achieving high AUC scores. This result highlights that the attack is feasible even on the FRTE benchmark using simple, open-source facial recognition models.[3]

The FRTE privacy vulnerability demonstrates how publicly releasing algorithmic benchmarking results can compromise the anonymity of individuals in private datasets. In the remainder of this paper, we focus on benchmarks where the private data used for evaluation is a graph, as graph datasets are common in fraud detection tasks and pose significant technical challenges.

[1] For a general binary query, the attacker would need an accurate estimator for that query given the private graph dataset.

[2] We have disclosed this vulnerability to NIST, which has implemented steps to reduce its exploitability. Moreover, note that this attack only reveals membership in the dataset—it does not reveal other information about the individuals in the gallery, such as date of the photo or biographic information.

[3] Our code and a detailed FRTE benchmark description are available at `https://github.com/akgoldberg/face_recognition_privacy_attack`.

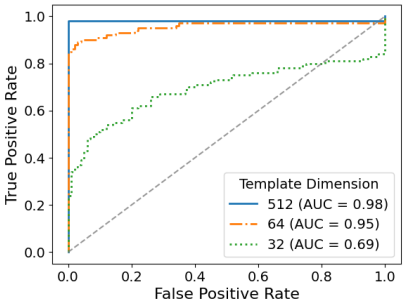


Figure 2: ROC curve of the privacy attack on NIST's FRTE benchmark, simulated on the CelebA dataset.

3 Problem Formulation

Based on the privacy risk posed by the attack in Section 2, we ask how to protect dataset privacy for the benchmarking server. We consider three different operating modes for the benchmarking server: (1) *one-shot*: the server releases the AUC score for a single submitted fraud detector, (2) *full leaderboard:* the server returns the AUC score for a set of submitted fraud detectors, and (3) *top-1 release:* the server releases the best-performing fraud detector among a set of submitted algorithms.

3.1 Incorporating Differential Privacy

We propose that the fraud benchmarking server satisfy a relaxation of differential privacy (DP) [10] that protects benign vertices:

Definition 3.1 (Protected differential privacy [23])**.** Two graphs G, G' are neighboring if:

(a) G and G' share the same partitions of fraudulent and non-fraudulent vertices V_1 and V_0.
(b) G can be obtained from G' by rewiring the edges of one *benign* vertex and/or changing that vertices' metadata.

Let f denote the benchmarking server that given a graph and fraud detector outputs an estimate of the AUC score. The server f satisfies ε-protected differential privacy if for any two neighboring graphs G, G', any fraud detection algorithm $\mathcal{A}$ and any possible set of outputs O:

$$\Pr[f(G, \mathcal{A}) \in O] \leq e^{\varepsilon} \Pr[f(G', \mathcal{A}) \in O].$$

Standard DP allows G and G' to differ in the data of *any* vertex in the graph, not just a benign vertex. Protected DP is a relaxation of standard DP in that any graphs that are neighbors per the definition of protected DP are also neighbors under standard DP. We will refer to protected differential privacy as DP for brevity throughout.

We primarily adopt this relaxed notion of privacy to improve utility. In many real-world graphs, the rate of fraud is low. Hence, requiring that the released accuracy statistic does not change much if we change the connections of these fraudulent vertices makes it difficult to release high-fidelity benchmarks. Still, we believe this relaxation is useful. In fraud detection, it is natural to hold different privacy expectations for fraudulent participants (many of which may even be fake [16]) compared to legitimate ones.

In the definition of neighboring graphs, we adopt the strong notion of *node* differential privacy, which protects all of the edges of any single benign vertex. Many prior works employ a weaker notion of *edge* differential privacy [4, 19, 21, 33], which defines neighboring graphs as graphs that differ in a single edge. We note that protected DP inherits the *composition property* of standard DP:

Theorem 3.1 (Composition [10]). *For any two fraud detectors $\mathcal{A}_1$ and $\mathcal{A}_2$, if releasing $f(\mathcal{A}_1, G)$ satisfies ε_1-protected DP and releasing $f(\mathcal{A}_2, G)$ satisfies ε_2-protected DP, then releasing both results on graph G, $(f(\mathcal{A}_1, G), f(\mathcal{A}_2, G))$ satisfies $(\varepsilon_1 + \varepsilon_2)$-DP.*

This property is helpful in moving from one-shot release of fraud detectors to releasing a leaderboard of many fraud detectors.

3.2 Challenges of Graph Data

Even evaluating a single fraud detector on graph data proves challenging under DP constraints. To understand why, let us compare our setting to evaluating a fraud detector on tabular data. Evaluating a single fraud detector can be seen as a problem of releasing a (noisy) query result. A simple mechanism that solves the query release problem adds random noise with variance scaled to the "sensitivity" of this query, which is defined as follows.

Definition 3.2 (Global Sensitivity)**.** For a query $f : \mathcal{X} \to \mathbb{R}^d$, define its *global sensitivity*

$$\Delta_f = \max_{G,G' \text{ neighbors}} \|f(G) - f(G')\|_1$$

as the worst-case change in f across any two neighboring graphs.

Then, a canonical mechanism, termed the Laplace Mechanism, scales noise to the global sensitivity:

Definition 3.3 (Laplace Mechanism [10])**.** On any input G the *Laplace Mechanism* with privacy parameter ε releases

$$\widetilde{f}(G) = f(G) + \text{Laplace}(\Delta_f/\varepsilon).$$

The Laplace Mechanism satisfies ε-DP.

In the tabular setting, model evaluation is a low sensitivity query and therefore can be released by directly applying the Laplace mechanism. Consider a simple case where fraud detector $\mathcal{A}$ is a fitted logistic regression model (the weights of the model are fixed). Changing any row of a tabular dataset changes at most a single fraud prediction score, so the AUC score of the fitted logistic regression can only change by $\frac{1}{n_0}$ by changing any row of the data. The Laplace mechanism can then release the true AUC score of the fraud detector plus Laplace noise with variance $\frac{2}{(\varepsilon n_0)^2}$.

In contrast, consider evaluating the logistic regression model on a graph where features of each vertex include graph statistics like the degree of each vertex. Because graph features depend on other vertices, changing any one vertex can change the features of all other vertices in the graph. In the worst-case, changing a vertex changes fraud prediction scores for all other vertices in the graph, so the AUC score has a large global sensitivity of 1. As this is the largest possible value AUC can take, the Laplace mechanism must add so much noise that the entire signal is lost.

In this paper, we focus on addressing this challenge of high sensitivity of model evaluation on graph data. In cases where queries

of a dataset have large worst-case sensitivity there are three classes of solutions in the DP literature:

(1) (*Subsample-and-aggregate*) Force low sensitivity of the AUC score by applying "subsample-and-aggregate."
(2) (*Synthetic data*) Generate DP synthetic data that captures some structure of the private graph and run fraud benchmarking on this private graph data.
(3) (*Calibrate noise to "local sensitivity."*) Estimate (an upper bound) on how sensitive f_{AUC} is on the specific graph and fraud detection algorithm $\mathcal{A}$ and calibrate noise to this sensitivity, which may be much lower than the worst case global sensitivity. This approach includes mechanisms like Propose-Test-Release, Smooth Sensitivity, and the Inverse Sensitivity Mechanism [11, 34] as well as recent work on privatizing black-box scripts run on private data [25].

We give instantiations of subsample-and-aggregate and synthetic data generation algorithms tailored to the benchmarking server setting and run extensive empirical evaluations to understand opportunities and shortcomings. We do not evaluate local sensitivity based methods [34], because these approaches are computationally infeasible in our setting as they would require enumerating every possible neighboring graph to estimate a bound on local sensitivity.

4 Related Work

To our knowledge, this work is the first to consider the problem of model evaluation on graph data under DP constraints. For tabular (non-graph) data, there are two lines of work that consider DP model evaluation. One line of work [2, 38, 46] proposes a framework of "verification servers" wherein analysts fit a model of data (e.g., a linear regression model) on a synthetic dataset and then employ a "verification server" which holds non-synthetic data to perform quality checks that their model is useful like goodness-of-fit tests. While the system design is similar, these works focus on tabular data rather than graph data, which poses specific challenges (Section 3.2).

A recent line of work in DP machine learning (starting with [30] and extended in [5, 36]), looks at a closely related problem of model selection under differential privacy constraints. These works focus on choosing the (nearly) optimal model in minimizing loss among a large set of models without paying for privacy loss that grows with the number of models. We observe that on graphs (even ignoring model training) the seemingly straightforward step of one-shot model evaluation is difficult under differential privacy constraints.

A number of works have considered the problem of running arbitrary queries on private data. Subsample-and-aggregate, first proposed in [34], is one popular method for reducing the sensitivity of a query. Practical instantiations of subsample-and-aggregate have been used in popular frameworks for data analysis as in GUPT [32] and for training ML models as in PATE [35]. In our work, we focus on model evaluation rather than training, as the model evaluation task is quite challenging in the graph setting. In contrast, to prior uses of subsample-and-aggregate, we propose up-sampling fraudulent entities satisfying a relaxed notion of privacy and improving utility. We then perform extensive empirical evaluation to understand how the subsample-and-aggregate framework compares to synthetic data generation algorithms for this problem. A recent work [25] also considers the problem of running arbitrary code on a private dataset and gives a new mechanism called TAHOE that is competitive with subsample-and-aggregate in some tabular data settings, but TAHOE is computationally expensive and and cannot run efficiently on graph data.

There is a long line of work in differentially private analysis of graph data. We discuss the literature on generating synthetic graphs in more detail in Section 6 where we detail our choice of synthetic graph algorithms to benchmark. These synthetic graph algorithms require estimating statistics of the graph (like degree distribution or number of triangles) under node differential privacy. This introduces new challenges as the prior works on synthetic data generation use the weaker notion of edge-DP to estimate statistics. In our work, we generically transform edge-DP estimation into (reasonably accurate) node-DP estimation using the idea of smoothly projecting a graph to the space of limited-degree graphs from [3, 22]. There may be additional improvements in applying existing synthetic data generation methods under the node-DP privacy regime by applying more tailored estimation procedures.

5 Subsample-and-Aggregate

The first approach we consider in privatizing fraud benchmarking is the subsample-and-aggregate framework [34]. Recall from Section 3.2 that a key challenge of releasing a DP estimate of the AUC score of a fraud detector on a graph is that this query has global sensitivity of 1, equal to the range of the AUC score. Subsample-and-aggregate forces low sensitivity of the query by partitioning the dataset into k disjoint sets and estimating AUC on each partition.

Our algorithm follows the template described above for benign vertices, that is, we partition the benign vertices into k disjoint sets of equal size. However, in fraud graphs, there are often very few fraudulent vertices. For example, in the Elliptic Bitcoin financial fraud dataset [43] there are only 11 fraudsters out of over $6,000$ vertices. Partitioning these fraud vertices into a reasonable number of partitions to achieve low sensitivity (say $k \geq 5$) would destroy any structure of the sub-graph of fraud vertices.

We therefore modify typical subsample-and-aggregate for the fraudulent vertices by allowing *duplication* of fraudsters across partitions. For each partition, we sample a subset of fraudulent vertices, where the rate of sub-sampling is controlled by a parameter ρ. We term this instance of subsample-and-aggregate as Partition, Duplicate, and Aggregate (PDA), described in Algorithm 2. Note that taking $\rho = 1$ results in duplicating all fraud vertices in each partition, while taking $\rho = \frac{1}{k}$ is similar to typical subsample-and-aggregate, but with the difference that fraudulent vertices may be sampled into multiple partitions.

It is straightforward to prove that Algorithm 2 guarantees differential privacy:

Proposition 5.1. *For any choice of sub-sampling rate $\rho \in (0, 1)$, number of partitions $k > 1$ and privacy parameter $\varepsilon > 0$, Algorithm 2 guarantees ε-Protected Differential Privacy (Definition 3.1).*

The proof follows from a standard proof of privacy for subsample-and-aggregate: changing the data of any benign vertex impacts at most 1 of the k partitions between any two neighboring graphs, and the accuracy score on this partition can change by at most 1 since f has global sensitivity (Definition 3.2) of 1. Hence, the mean across partitions has global sensitivity of $\frac{1}{k}$ and privacy follows

Algorithm 2 Partition, Duplicate, and Aggregate

Parameters: privacy parameter $\varepsilon > 0$, number of partitions k, fraud sub-sampling rate ρ.
Inputs: fraud detector $\mathcal{A}$, accuracy statistic f with global sensitivity Δ, fraud vertices V_1, benign vertices V_0, graph G on vertex set $V_0 \cup V_1$.

- Randomly partition non-fraud nodes V_1 into k equally size sets $V_0^{(1)}, \ldots, V_0^{(k)}$.
- Randomly sample k sets of fraud nodes $V_1^{(1)}, \ldots, V_1^{(k)}$ where each $V_1^{(i)}$ is sampled independently uniformly from all sub-sets of V_1 of size $\rho \cdot |V_1|$.
- Let $G_1, \cdots, G_k$ be sub-graphs of G on vertices $(V_0^{(1)} \cup V_1^{(1)}), \ldots, (V_0^{(k)} \cup V_1^{(k)})$.
- Release $Z + \frac{1}{k}\sum_{i=1}^{k} f(\mathcal{A}, G_i)$ where $Z \sim \text{Laplace}(\Delta/(k\varepsilon))$.

from the Laplace mechanism (Definition 3.3). We note that in practice, the subsample-and-aggregate framework does not introduce substantial computational overhead.

5.1 Running Multiple Benchmarks

Algorithm 2 provides a method for one-shot release of the AUC score of a single fraud detector. In order to apply it to full leaderboard release, we can invoke composition (Theorem 3.1) and subdivide the privacy budget among many fraud detectors. For example, if we have 10 algorithms to benchmark, we run each with privacy budget of $\varepsilon/10$ per fraud detector. As it is harder to provide good utility for smaller ε, we expect our accuracy of estimation to degrade in the number of detectors benchmarked.

In many real-world settings it is useful to release only the best or the top-m fraud detectors, for example when running a competition. In the case of top-1 release, we can use the *Report Noisy Arg Max* mechanism [12]. This mechanism adds Laplace noise to any (finite) number of queries as per the Laplace mechanism, but then only releases the name of the query with the largest (noisy) value. Rather than paying composition cost that grows in the number of queries, this procedure is ε-DP. In our case, then, we can apply Algorithm 2 to arbitrarily many fraud detectors and then at the end only publicly release the name of the detector with the highest noisy AUC score. This guarantees ε-DP when each run of Algorithm 2 is run using privacy parameter ε. While we do not experiment with releasing the top-m fraud detectors, recent work [37] shows that releasing the top-m fraud detectors ranked by noisy AUC (among a larger set of fraud detectors) only incurs total privacy loss of $m\varepsilon$.

6 Synthetic Data Generation

In this section, we describe our choice of synthetic graph data generation algorithms to benchmark; the surveys [15, 28] provide a useful overview of such algorithms. Many methods do not handle *labeled* vertices. Such methods cannot be applied to our problem, as synthetic data for fraud detection benchmarking needs to differentiate between fraudulent and benign vertices. Additionally, most existing work focuses on satisfying the weaker notion of edge-level DP, while we wish to satisfy node-level DP. Therefore, we focus on the following 3 methods that all handle labelled vertices and are amenable to transformation into a node-level DP algorithm:

(1) *Stochastic block model (SBM)*: Estimate a stochastic block model with two communities (fraud and non-fraud) and sample a graph based on the SBM parameters. For a fixed number of benign and fraud vertices, the stochastic block model has three parameters p_1, p_0, p_{01}. Each edge in the graph is sampled independently at random with probability p_1 if both of its endpoints are fraudulent, p_0 if both are benign, and p_{01} if one is fraudulent and the other is benign.
(2) *Attributed social graph* (ASG): [19]: Estimate the connection probabilities with and between fraud and non-fraud vertices (as in the SBM), but additionally estimate number of triangles in the graph and the degree sequence of the graph. Then, sample a graph that matches these noisy statistics. We run two versions of this method, with and without the triangle statistic.
(3) *Top-m-filter* [33]: Directly perturb the adjacency matrix of the graph. In particular, flip each edge in the graph and then perform a filtering step to remove edges to match a noisy estimate of total number of edges.

In general, synthetic data methods first compute graph statistics under differential privacy, which provide a succinct representation of the graph, and then generate the synthetic graph based on these (noisy) statistics. More expressive graph models may better represent the graph structure, but tend to require the estimation of noisier sufficient statistics due to differential privacy. We choose methods that lie along this spectrum of model complexity.

Other popular synthetic data methods in the literature use exponential random graph models (ERGMs) and more recently graph neural networks (GNNs) [45, 47]. These methods are either computationally intractable for large graphs in the case of ERGMs or would require too much noise addition when fitting GNNs under node-level privacy.

Guaranteeing Node-Level Differential Privacy. The algorithms we consider were designed to provide edge-level differential privacy. In privately computing sufficient statistics of the graph, these algorithms add Laplace noise proportional to the worst-case sensitivity of a statistic to the change of a single edge in a graph. In order to guarantee node-level privacy in this noise addition step, we use the idea of projecting the graph to the space of graphs with bounded maximum degree from [3, 22] and then adding noise proportional to this "restricted sensitivity." For a given graph G, choice of truncation threshold T, and graph statistic g, the full workflow is:

(1) (Naive truncation). Truncate graph G by removing all vertices with degree above D.
(2) Estimate the "smooth sensitivity" S of the naive truncation operation per [22].[4]
(3) Add Laplace noise with scale proportional to $S \cdot RS_T(g)$ where $RS_T(g)$ represents the "restricted sensitivity" of g on graphs of max degree D, that is the maximum change in g between any two node-adjacent graphs of max degree T.

[4] From [22], Proposition 6.1 we can compute the smooth sensitivity $S^{\beta}_{trunc}(G,T)$ of the truncation operation as follows. Let $N_t(G,T)$ denote the number of benign vertices with degree in range $[T-t, T+t+1]$ and $C_t(G,T) = 1 + t + N_t(G,T)$. Then, $S^{\beta}_{trunc}(G,T) = \max_{t\geq 0} e^{-\beta t} C_t(G,T)$.

We summarize the framework for node-private synthetic data release in Algorithm 3. Since the max degree and average degree of the fraud graphs used (see Table 1) tends to be much smaller than the number of vertices in the graph, the restricted sensitivity tends to be much lower than the global sensitivity.

Note that using this method with Laplace noise actually guarantees the relaxation of (ϵ, δ)-differential privacy due to the use of "smooth sensitivity" [34]. We fix δ to 10^{-8} for all experiments on synthetic data methods. Additionally, to provide a fair comparison against our subsample-and-aggregate method which relaxes privacy for fraudulent vertices, we compute statistics that rely only on the fraudulent nodes without noise.

Algorithm 3 Framework for Node-Private Synthetic Data Release

Parameters: privacy parameters $\varepsilon > 0, \delta \in (0,1)$, degree threshold T

Inputs: fraud vertices V_1, benign vertices V_0, graph G on vertex set $V_0 \cup V_1$, vector of sufficient statistics to compute $g(G)$ with restricted sensitivity Δ_T.

- Remove all benign vertices from G with degree greater than T.
- Compute the β-smooth sensitivity $S^{\beta}_{trunc}(G,T)$ of the truncation operation on G, where $\beta = -\frac{2\varepsilon}{\log(1/2\delta)}$.
- Release $\widetilde{g}(G) = g(G) + Z$ where $Z \sim \text{Laplace}(2S^{\beta}_{trunc}(G,T) \cdot \Delta_T/\varepsilon)$.
- Sample output synthetic graph $\widetilde{G}$ based on $\widetilde{g}(G)$.

7 Experimental Setup

We now describe our datasets, fraud detectors, and metrics.

7.1 Datasets

We test methods for fraud benchmarking on 4 datasets representing a variety of domains and graph structures. All graphs are undirected unipartite graphs. In *Yelp* [9] and *Amazon* [9] each vertex represents a reviewer with edges denoting common reviews on the products/restaurants and fraudulent reviewers represent spammers and low-rated reviewers respectively. *Peer Review* consists of paper reviewers at a computer science conference with edges denoting mutual bids on each other's papers [44]. Following [16] we inject a clique of 22 fraudulent reviewers with edge density of 0.8 among these reviewers into the graph, which corresponds to the smallest injected clique that was possible to detect in prior work. Finally, in *Elliptic* [43] each vertex in the graph represents a transaction from the Bitcoin blockchain, an edge represents a flow of Bitcoins between one transaction and the other, and fraudulent nodes are illicit transactions. We take a single time-step from the entire Elliptic graph (summary statistics in Table 1 in Appendix A).

We run analyses of subsample-and-aggregate and synthetic data algorithms on validation datasets to understand settings of hyperparameters before comparing these methods against each other. We use four validation datasets. For Yelp, we use a random split of the vertices with 11k vertices in the test set and 11k in the validation set. For Elliptic, we use different disjoint time periods for validation and test. For Amazon and Peer Review, there are not standard train-test splits used in past work. We therefore use the entire graph for evaluation, and generate validation graphs to set hyperparameters by estimating parameters of a stochastic block model (SBM) and sampling from this model.

7.2 Fraud Detectors

We evaluate 10 simple fraud detectors that do not require learning, and 3 detectors that learn on a subset of the benchmark data. Specifically we evaluate the following fraud detectors:

- *(Negative) Degree [17]*: rank by the degree of each vertex.
- *(Negative) Clustering Coefficient*: rank by the clustering coefficient of each vertex, inspired by [1].
- *SVD Error [17]*: take the singular value decomposition of the adjacency matrix to obtain a low rank approximation (for specified rank r). Then, rank each vertex by reconstruction error (aggregating over edges by taking either the sum or the max over edges). We use $r = 10$ for the sum and $r = 50$ for the max, chosen to maximize average AUC across all datasets in a grid search.
- *Community Detection*: run Leiden community detection [40] to place cluster vertices in a cluster and rank by cluster size (with larger clusters less likely to be fraudulent).
- *Aggregations:* take weighted averages of the (normalized) scores or maximum scores obtained from subsets of the prior methods.
- *GraphSAGE (SAGE) [14]*: learns a function that aggregates embeddings from neighboring nodes to learn a node embedding for each vertex and uses these embeddings to predict fraud labels.
- *Graph Convolutional Network (GCN) [24]*: learns node representations by applying a layer-wise convolutional operation that aggregates and normalizes features from immediate neighbors.
- *Graph Attention Network (GAT) [41]*: employs attention mechanisms to weight the influence of neighboring nodes during aggregation.

The last three detectors involve a learning component; we trained each GNN on a random 80% of vertices and then assessed AUC score on the held-out 20%. These algorithms give a wide range of AUC scores on each dataset. For example, on Yelp, GCN performs the best with an AUC score of 0.73 and SVD Error (Sum) performs poorly with an AUC score of 0.34. In contrast, on Peer Review, SVD Error (Sum) performs the best with an AUC score of 0.88, while Neg Degree has very bad performance with AUC of 0.12.

7.3 Measuring Utility

We consider three metrics to compare utility across methods. Each metric corresponds to one of the release modes for the benchmarking server: one-shot, full leaderboard and top-1 release. Let $\{\mathcal{A}_i\}_{i=1}^m$ denote a set of m fraud detectors to benchmark on graph G, $f_{\text{AUC}}(\mathcal{A}_i, G)$ denote the true AUC score for fraud detector i on G and $\tilde{f}_{\text{AUC}}(\mathcal{A}_i, G)$ denote the noisy DP estimate of the AUC score. For the one-shot release, where we wish to release AUC for a single fraud detector, we calculate *L1 error*: $|f_{\text{AUC}}(\mathcal{A}_i, G) - \tilde{f}_{\text{AUC}}(\mathcal{A}_i, G)|$.

When evaluating top-1 release of the best fraud detector among a set of fraud detectors we measure utility by the distance between the true AUC of the true best fraud detector (computed without any privacy) and the true AUC of the released best fraud detector. That is, we define top-1 error as:

$$f_{\text{AUC}}(\mathcal{A}_{top}, G) - f_{\text{AUC}}(\mathcal{A}_{top'}, G) \text{ where } top = \sigma^{-1}(1), top' = \widetilde{\sigma}^{-1}(1).$$

For the full leaderboard setting we use the weighted Kendall-Tau distance between rankings [27]. We discuss this metric and provide results in this setting in Appendix B.2.

In addition to using the AUC score as an accuracy metric, we evaluate the F1 score of fraud detectors, another popular measure of fraud detector accuracy. We find similar results to that of AUC score, but F1 score tends to be even more difficult to release accurately. We present these additional results in the arXiv version of this paper.

8 Experimental Results

In this section we provide results of our comparison of Subsample-and-Aggregate and Synthetic Graph Generation (8.1), and experiments to understand trade-offs between distorting graph structure and adding noise to preserve privacy for Subsample-and-Aggregate (8.2) and Synthetic Graph Generation (8.3).

8.1 Comparison of Algorithms

We benchmark subsample-and-aggregate against synthetic data algorithms for the concrete task of releasing the best fraud detectors among a set of fraud detectors. We choose parameters of subsample-and-aggregate (number of partitions and sub-sampling rate) based on the best parameters for each dataset in releasing a ranking of all fraud detectors on the validation dataset. This follows prior work [32], which assumes access to public datasets from which one could estimate subsample-and-aggregate hyperparameters.

In Figure 1, we show results of the DP benchmarking methods for top-1 release. We decompose the error into *inductive bias* from how a method distorts graph structure, and error from the addition of *privacy-preserving random noise*. To visualize this, we plot each method without privacy-preserving noise on the x-axis and with noise needed to preserve privacy on the y-axis. Specifically, for Non-Private subsample-and-aggregate we only apply the graph partitioning and do not add Laplace noise to the AUC score. For non-private synthetic data methods we compute sufficient statistics for each method without any noise addition and then generate a graph using those sufficient statistics. Among synthetic data methods, Topmfilter has no error without privacy as it releases the full adjacency matrix, while SBM and AGM introduce error even without privacy. However, after adding noise needed for privacy, SBM performs the best among synthetic data methods. Perhaps surprisingly, this is true even for GNN-based fraud detectors as shown in Figure 5. Subsample-and-aggregate distorts graph structure extensively, even with only 5 partitions, resulting in high error without privacy. We provide additional results for larger privacy budget and other datasets in Appendix B.1, but the general trends are similar.

8.2 Subsample-and-Aggregate

In experiments on four validation datasets, we seek to understand how the parameters of the algorithm—number of partitions k and rate of sub-sampling fraud in each partition ρ—impact the bias, variance from Laplace noise addition and overall distortion of fraud detector rankings.

On each dataset we run Algorithm 2 for 10 trials for each choice of parameters k, ρ and ε. We show per-dataset results on the Yelp and Elliptic validation datasets in this section. We provide additional results on Amazon and Peer Review in Appendix B.3.

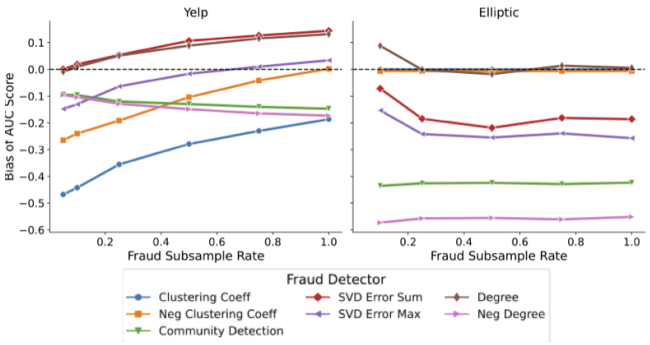


Figure 3: Bias to the AUC score introduced by subsample-and-aggregate for each fraud detector varying the fraud subsample rate (ρ) while fixing number of partitions $k = 20$. Subsample-and-aggregate introduces extensive bias to all fraud detectors, with the sign and magnitude of the bias varying widely across fraud detectors.

In general, we find that partitioning the graph into random subgraphs introduces significant bias to estimates of graph statistics. The sign and magnitude of this bias can differ widely across fraud detectors. In Figure 3, we show bias per fraud detector fixing the number of partitions at $k = 20$ and varying the fraud sub-sampling rate. We find that it is not always possible to achieve zero bias for a given fraud detector for a given number of partitions $k = 20$. For instance, the clustering coefficient detector has negative bias on the Yelp dataset at all values of ρ. This makes sense as removing benign vertices from the graph may change the distribution of fraud detection scores for benign vertices such that it is not possible to recover a similar distribution at any rate of sub-sampling fraudulent vertices. We additionally find, as expected, that the magnitude of bias increases with the number of partitions (k) although the sign of the bias differs across fraud detectors. We plot bias as a function of number of partitions in Figure 12 of Appendix B.3. These results explain the poor performance of subsample-and-aggregate in Figure 1, as subsampling tends to distort graph structure extensively, biasing different fraud detectors in different ways thereby undermining the utility of the ranking of fraud detectors.

8.3 Synthetic Graph Generation

In our experiments we aim to isolate error introduced due to choice of graph model and noisy estimation of sufficient statistics. For each synthetic data generation algorithm, we generate 10 synthetic data sets. For each synthetic graph method, we subdivide the privacy budget evenly between the different parameters to estimate. We note that it may be possible to better distribute privacy budget between different statistics, which is an interesting area for future investigation. We test degree truncation thresholds as a function of the max degree of each graph, so 1.0 is a threshold exactly equal to the maximum degree benign vertex in a graph while 0.5 removes all nodes with degree > 0.5 times the max degree. In this section, we report results with threshold of 1 and give additional results for 0.5 in Appendix B.4.

	# Edges	Degree Sequence	# Triangles	Adjacency Matrix
Yelp	0.01	1.26	0.99	1.93
Elliptic	17.61	20.94	117.11	1.84
Amazon (SBM)	0.01	0.47	0.84	1.94
Peer Review (SBM)	0.21	1.34	22.69	1.95

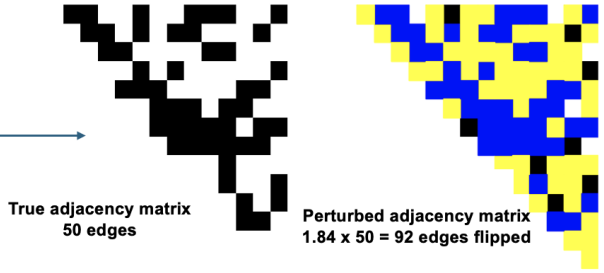


Figure 4: Normalized mean absolute error (MAE) introduced to each of the synthetic graph sufficient statistics. We fix $\varepsilon = 5.0$ and the degree cutoff to $1\times$ the graph's max degree. It is possible to estimate SBM parameters accurately, while other parameters have large noise addition. We give an example of what relative error of 1.84 means for the adjacency matrix on the right, where an adjacency matrix with 50 edges has 92 edges flipped: 42 removed (yellow) and 50 added (blue.)

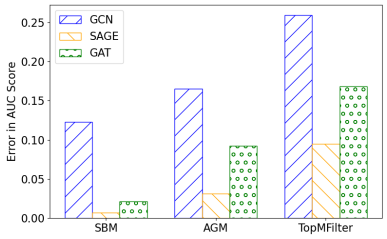


Figure 5: Error in AUC score for GNN-based fraud detectors on Yelp data using synthetic graphs with $\varepsilon = 5.0$.

We find that outside of the SBM, it is necessary to introduce large distortion to the sufficient statistics of each graph model in order to preserve privacy, as shown in Figure 4. We show the proportional change in each noisy sufficient statistic compared to its true value, taking the mean over a vector-valued statistic. On Yelp, Amazon, and Peer Review it is possible to estimate the edge count for the SBM with high accuracy at $\varepsilon = 5.0$, perturbing the edge count by 1% of the total number on Yelp and Amazon. Elliptic is an extremely sparse graph (0.04%), so we introduce much larger relative error. For degree sequence and number of triangles, the amount of error is one to two orders of magnitude larger, with error generally at least 50% of the value of the original statistic. Unsurprisingly, the adjacency matrix cannot be accurately estimated under node-DP via direct noise addition. We highlight the amount of noise addition needed to preserve privacy in a simple example of relative error of 1.84 on a 15x15 adjacency matrix, shown in Figure 4. Even after aggressively truncating high-degree nodes, the addition of DP noise results in flipping the same number of edges as were originally in the adjacency matrix. This large distortion of sufficient statistics explains the poor accuracy of AGM and TopMfilter.

9 Discussion

In this work we define the novel problem of privately benchmarking fraud detectors on graph-structured data. We benchmark two popular frameworks from the DP literature, subsample-and-aggregate and synthetic data generation. We characterize a trade-off for each method between error arising from bias due to distorting graph structure and error arising from privacy-preserving noise addition. Our results suggest the need to develop methods that trade-off more effectively between graph distortion and noise addition. There are a number of open directions in moving towards this goal:

(1) *Model / hyper-parameter selection under privacy constraints:* Our experiments suggest that choice of hyperparameters (e.g., number of partitions in subsample-and-aggregate) and more generally method can have a large impact on utility, raising the problem of how to choose the model and hyper-parameters privately.
(2) *General vs. tailored methods of synthetic graph generation:* There are not existing DP synthetic graph algorithms specifically tailored to fraud detection. In our experiments, we find that existing methods introduced significant bias even without noisy sufficient statistics, suggesting that these models do not capture the structure of graphs needed to model fraudulent behavior.
(3) *Modeling synthetic graph meta-data:* Existing synthetic graph methods try to directly model graph structure. Our experiments demonstrate that this is challenging due to the sensitivity of many graph statistics. We hypothesize that modeling graph meta-data can lead to more effective DP synthetic graph generation methods as meta-data is attributable to one vertex and can therefore be modeled as tabular data. Then, connectivity between vertices could be estimated using lower sensitivity edge counts between clusters of vertex features as in an SBM.

In conclusion, our work highlights privacy vulnerabilities in benchmarking fraud detectors on private data and explores the challenges in balancing privacy and utility on graph-structured data.

Acknowledgments

We thank Patrick Grother and Craig Watson of NIST for constructive discussion and comments. A. Goldberg and G. Fanti acknowledge the Air Force Office of Scientific Research under award number FA9550-21-1-0090, NSF grant CNS-2148359, the Bill & Melinda Gates Foundation, Intel, and the Sloan Foundation for their generous support. A. Goldberg and N. Shah acknowledge the support of NSF grant 2200410 and ONR grant N000142212181. S. Wu acknowledges the support of NSF grant 2232693.

References

[1] Leman Akoglu, Mary McGlohon, and Christos Faloutsos. 2010. Oddball: Spotting anomalies in weighted graphs. In *Advances in Knowledge Discovery and Data Mining: 14th Pacific-Asia Conference, PAKDD 2010, Hyderabad, India, June 21-24, 2010. Proceedings. Part II 14*. Springer, 410–421.

[2] Andrés F Barrientos, Aaron R Williams, Joshua Snoke, and CM Bowen. 2021. *Differentially Private Methods for Validation Servers*. Technical Report. Urban Institute research report.

[3] Jeremiah Blocki, Avrim Blum, Anupam Datta, and Or Sheffet. 2013. Differentially private data analysis of social networks via restricted sensitivity. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science* (Berkeley, California, USA) *(ITCS '13)*. Association for Computing Machinery, New York, NY, USA, 87–96. https://doi.org/10.1145/2422436.2422449

[4] Xihui Chen, Sjouke Mauw, and Yunior Ramírez-Cruz. 2019. Publishing Community-Preserving Attributed Social Graphs with a Differential Privacy Guarantee. *Proceedings on Privacy Enhancing Technologies* 2020 (2019), 131 – 152. https://api.semanticscholar.org/CorpusID:202540124

[5] Edith Cohen, Xin Lyu, Jelani Nelson, Tam'as Sarl'os, and Uri Stemmer. 2022. Generalized Private Selection and Testing with High Confidence. *ArXiv* abs/2211.12063 (2022). https://api.semanticscholar.org/CorpusID:253761282

[6] Federal Trade Commission. 2024. As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public. https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public. (Accessed on 02/29/2024).

[7] Datavisor. 2024. Datavisor: AI Powered Fraud Platform for Enterprise. https://www.datavisor.com/ (Accessed on 02/29/2024).

[8] Jiankang Deng, Jia Guo, Niannan Xue, and Stefanos Zafeiriou. 2019. Arcface: Additive angular margin loss for deep face recognition. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 4690–4699.

[9] Yingtong Dou, Zhiwei Liu, Li Sun, Yutong Deng, Hao Peng, and Philip S. Yu. 2020. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management* (Virtual Event, Ireland) *(CIKM '20)*. Association for Computing Machinery, New York, NY, USA, 315–324. https://doi.org/10.1145/3340531.3411903

[10] Cynthia Dwork. 2006. Differential Privacy. In *Automata, Languages and Programming*, Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–12.

[11] Cynthia Dwork and Jing Lei. 2009. Differential privacy and robust statistics. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing* (Bethesda, MD, USA) *(STOC '09)*. Association for Computing Machinery, New York, NY, USA, 371–380. https://doi.org/10.1145/1536414.1536466

[12] Cynthia Dwork and Aaron Roth. 2014. The Algorithmic Foundations of Differential Privacy. *Found. Trends Theor. Comput. Sci.* 9, 3–4 (aug 2014), 211–407. https://doi.org/10.1561/0400000042

[13] Prince Grover, Julia Xu, Justin Tittelfitz, Anqi Cheng, Zheng Li, Jakub Zablocki, Jianbo Liu, and Hao Zhou. 2023. Fraud Dataset Benchmark and Applications. arXiv:2208.14417 [cs.LG]

[14] Will Hamilton, Zhitao Ying, and Jure Leskovec. 2017. Inductive representation learning on large graphs. *Advances in neural information processing systems* 30 (2017).

[15] Y. Hu, F. Wu, Q. Li, Y. Long, G. Garrido, C. Ge, B. Ding, D. Forsyth, B. Li, and D. Song. 2024. SoK: Privacy-Preserving Data Synthesis. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 2–2. https://doi.org/10.1109/SP54263.2024.00002

[16] Steven Jecmen, Nihar B. Shah, Fei Fang, and Leman Akoglu. 2024. On the Detection of Reviewer-Author Collusion Rings From Paper Bidding. arXiv:2402.07860 [cs.SI]

[17] Steven Jecmen, Minji Yoon, Vincent Conitzer, Nihar B. Shah, and Fei Fang. 2022. A Dataset on Malicious Paper Bidding in Peer Review. https://doi.org/10.48550/ARXIV.2207.02303

[18] Shouling Ji, Prateek Mittal, and Raheem Beyah. 2017. Graph Data Anonymization, De-Anonymization Attacks, and De-Anonymizability Quantification: A Survey. *IEEE Communications Surveys & Tutorials* 19, 2 (2017), 1305–1326. https://doi.org/10.1109/COMST.2016.2633620

[19] Zach Jorgensen, Ting Yu, and Graham Cormode. 2016. Publishing Attributed Social Graphs with Formal Privacy Guarantees. In *Proceedings of the 2016 International Conference on Management of Data* (San Francisco, California, USA) *(SIGMOD '16)*. Association for Computing Machinery, New York, NY, USA, 107–122. https://doi.org/10.1145/2882903.2915215

[20] Kaggle. 2024. Kaggle: Your Machine Learning and Data Science Community. https://www.kaggle.com/ (Accessed on 02/29/2024).

[21] Vishesh Karwa, Sofya Raskhodnikova, Adam Smith, and Grigory Yaroslavtsev. 2014. Private Analysis of Graph Structure. *ACM Trans. Database Syst.* 39, 3, Article 22 (oct 2014), 33 pages. https://doi.org/10.1145/2611523

[22] Shiva Prasad Kasiviswanathan, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. 2013. Analyzing Graphs with Node Differential Privacy. In *Theory of Cryptography*, Amit Sahai (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 457–476.

[23] Michael Kearns, Aaron Roth, Zhiwei Wu, and Grigory Yaroslavtsev. 2016. Private algorithms for the protected in social network search. *Proceedings of the National Academy of Sciences* 113 (01 2016), 201510612. https://doi.org/10.1073/pnas.1510612113

[24] Thomas N Kipf and Max Welling. 2016. Semi-supervised classification with graph convolutional networks. *arXiv preprint arXiv:1609.02907* (2016).

[25] Nitin Kohli and Paul Laskowski. 2023. Differential Privacy for Black-Box Statistical Analyses. *Proceedings on Privacy Enhancing Technologies* 3 (2023), 418–431.

[26] Kount. 2024. Kount: Fraud Detection and Chargeback Management Solutions. https://kount.com/ (Accessed on 02/29/2024).

[27] Ravi Kumar and Sergei Vassilvitskii. 2010. Generalized distances between rankings. In *Proceedings of the 19th International Conference on World Wide Web* (Raleigh, North Carolina, USA) *(WWW '10)*. Association for Computing Machinery, New York, NY, USA, 571–580. https://doi.org/10.1145/1772690.1772749

[28] Yang D. Li, Michaela F. Purcell, Thierry Rakotoarivelo, David B. Smith, Thilina Ranbaduge, and Kee Siong Ng. 2021. Private Graph Data Release: A Survey. *Comput. Surveys* 55 (2021), 1 – 39.

[29] Michael L Littman. 2021. Collusion rings threaten the integrity of computer science research. *Commun. ACM* 64, 6 (2021), 43–44.

[30] Jingcheng Liu and Kunal Talwar. 2018. Private Selection from Private Candidates. arXiv:1811.07971 [cs.DS]

[31] Ziwei Liu, Ping Luo, Xiaogang Wang, and Xiaoou Tang. 2015. Deep Learning Face Attributes in the Wild. In *Proceedings of International Conference on Computer Vision (ICCV)*.

[32] Prashanth Mohan, Abhradeep Thakurta, Elaine Shi, Dawn Song, and David Culler. 2012. GUPT: privacy preserving data analysis made easy. In *Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data*. 349–360.

[33] Hiep H. Nguyen, Abdessamad Imine, and Michaël Rusinowitch. 2015. Differentially Private Publication of Social Graphs at Linear Cost. In *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015* (Paris, France) *(ASONAM '15)*. Association for Computing Machinery, New York, NY, USA, 596–599. https://doi.org/10.1145/2808797.2809385

[34] Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. 2007. Smooth Sensitivity and Sampling in Private Data Analysis. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing* (San Diego, California, USA) *(STOC '07)*. Association for Computing Machinery, New York, NY, USA, 75–84. https://doi.org/10.1145/1250790.1250803

[35] Nicolas Papernot, Shuang Song, Ilya Mironov, Ananth Raghunathan, Kunal Talwar, and Úlfar Erlingsson. 2018. Scalable Private Learning with PATE. arXiv:1802.08908 [stat.ML]

[36] Nicolas Papernot and Thomas Steinke. 2021. Hyperparameter Tuning with Renyi Differential Privacy. *ArXiv* abs/2110.03620 (2021). https://api.semanticscholar.org/CorpusID:238419564

[37] Gang Qiao, Weijie Su, and Li Zhang. 2021. Oneshot Differentially Private Top-k Selection. In *Proceedings of the 38th International Conference on Machine Learning (Proceedings of Machine Learning Research, Vol. 139)*, Marina Meila and Tong Zhang (Eds.). PMLR, 8672–8681. https://proceedings.mlr.press/v139/qiao21b.html

[38] Jerome P Reiter, Anna Oganian, and Alan F Karr. 2009. Verification servers: Enabling analysts to assess the quality of inferences from public use data. *Computational Statistics & Data Analysis* 53, 4 (2009), 1475–1482.

[39] Riskified. 2024. Riskified: Fraud Prevention & Chargeback Fraud Protection. https://www.riskified.com/ (Accessed on 02/29/2024).

[40] Vincent A Traag, Ludo Waltman, and Nees Jan Van Eck. 2019. From Louvain to Leiden: guaranteeing well-connected communities. *Scientific reports* 9, 1 (2019), 5233.

[41] Petar Velickovic, Guillem Cucurull, Arantxa Casanova, Adriana Romero, Pietro Lio, Yoshua Bengio, et al. 2017. Graph attention networks. *stat* 1050, 20 (2017), 10–48550.

[42] T. N. Vijaykumar. 2020. Potential Organized Fraud in ACM/IEEE Computer Architecture Conferences. https://medium.com/@tnvijayk/potential-organized-fraud-in-acm-ieee-computer-architecture-conferences-ccd61169370d.

[43] Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I. Weidele, Claudio Bellei, Tom Robinson, and Charles E. Leiserson. 2019. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. arXiv:1908.02591 [cs.SI]

[44] Ruihan Wu, Chuan Guo, Felix Wu, Rahul Kidambi, Laurens van der Maaten, and Kilian Q. Weinberger. 2021. Making Paper Reviewing Robust to Bid Manipulation Attacks. In *Proceedings of the 38th International Conference on Machine Learning, ICML 2021, 18-24 July 2021, Virtual Event (Proceedings of Machine Learning Research, Vol. 139)*, Marina Meila and Tong Zhang (Eds.). PMLR, Virtual Event, 11240–11250. http://proceedings.mlr.press/v139/wu21b.html

[45] Minji Yoon, Yue Wu, John Palowitch, Bryan Perozzi, and Russ Salakhutdinov. 2023. Graph generative model for benchmarking graph neural networks. In

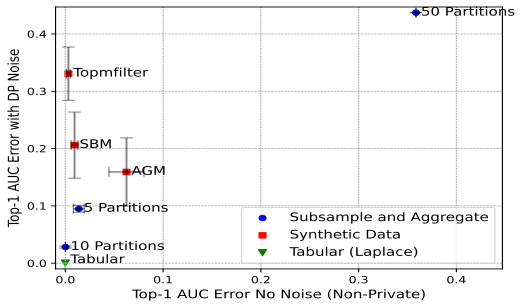


Figure 6: Top-1 AUC, $\varepsilon = 5.0$ on Elliptic Data

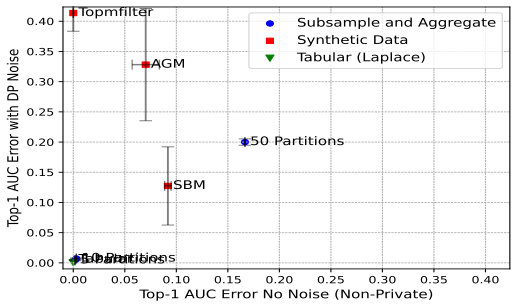


Figure 7: Top-1 AUC, $\varepsilon = 5.0$ on Peer Review Data

Proceedings of the 40th International Conference on Machine Learning (ICML'23). JMLR.org, , Honolulu, Hawaii, USA„ Article 1680, 24 pages.

[46] Haoyang Yu and Jerome P Reiter. 2018. Differentially Private Verification of Regression Predictions from Synthetic Data. *Trans. Data Priv.* 11, 3 (2018), 279–297.

[47] Kiarash Zahirnia, Yaochen Hu, Mark Coates, and Oliver Schulte. 2024. Neural Graph Generation from Graph Statistics. *Advances in Neural Information Processing Systems* 36 (2024).

A Summary of Datasets

	Yelp	Amazon	Peer Review	Elliptic
Vertices	11,473	11,944	2,483	6,621
Edge Density (%)	0.41	6.17	0.77	0.04
Num Fraud	1,657	821	22	11
Max Degree	236	6,991	255	47
Mean Degree	47.45	736.50	19.12	2.51

Table 1: Graph test datasets

B Additional Results

In this section we present additional results of our experiments.

B.1 Comparison of Algorithms, Top-1 Release

In Figures 6 and 7, we show the same plot as Figure 1 for the Elliptic and Peer Review datasets. In Figures 8, 9, **??**, and **??**, we give results for the stricter privacy budget of $\varepsilon = 2.0$.

B.2 Comparison of Algorithms, Full Leaderboard

For the full leaderboard, to capture distance between the true ranking of fraud detectors and the privacy-preserving noisy ranking, we use a similarity-weighted Kendall-Tau distance [27], which counts the number of inversions between two rankings, weighted by the difference in true AUC scores of the swap. Precisely, let $\sigma(i)$ denote the rank of fraud detector $\mathcal{A}_i$ in the true AUC leaderboard and $\widetilde{\sigma}(i)$ denote the rank of fraud detector $\mathcal{A}_i$ in the noisy AUC leaderboard. Then, the similarity weighted Kendall-Tau distance is given by:

$$\sum_{(i,j):\sigma(i)<\sigma(j)} \mathbb{1}\left[\widetilde{\sigma}(i) > \widetilde{\sigma}(j)\right] \left(f_{\text{AUC}}(\mathcal{A}_i, G) - f_{\text{AUC}}(\mathcal{A}_j, G)\right).$$

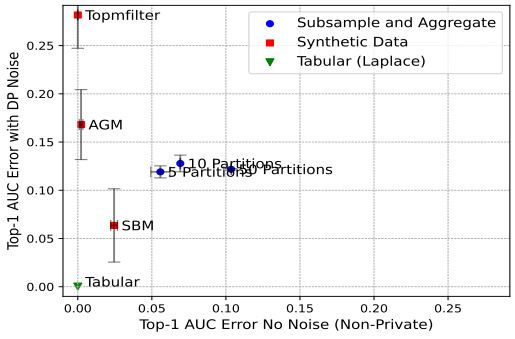


Figure 8: Top-1 AUC, $\varepsilon = 2.0$ on Amazon Data

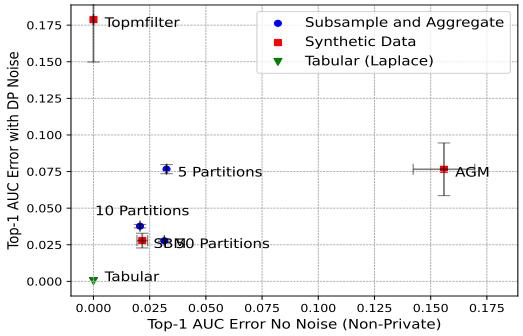


Figure 9: Top-1 AUC error, $\varepsilon = 2.0$ on Yelp Data

As a baseline value for the Kendall-Tau similarity on our set of 10 fraud detectors on each dataset, we can compute the expected distance between the true leaderboard and a random permutation of the fraud detectors for each dataset. This yields values in the range of 5 to 8 for each dataset (which we show as baselines in our results section). For further validation of the metric, we consider the distance between rankings on validation and test sets for the Yelp and Elliptic datasets. We find that the distance from test to

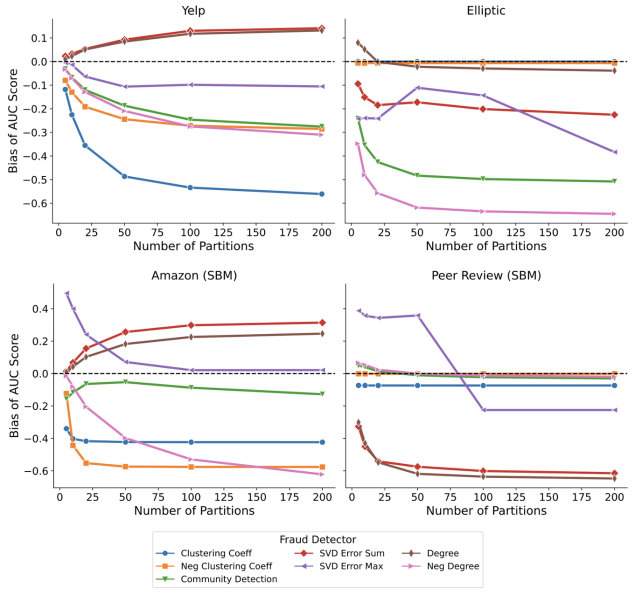


Figure 12: Bias to the AUC score introduced by subsample-and-aggregate for each fraud detector varying the number of partitions (k) while fixing fraud sub-sampling rate of $\rho = 0.5$.

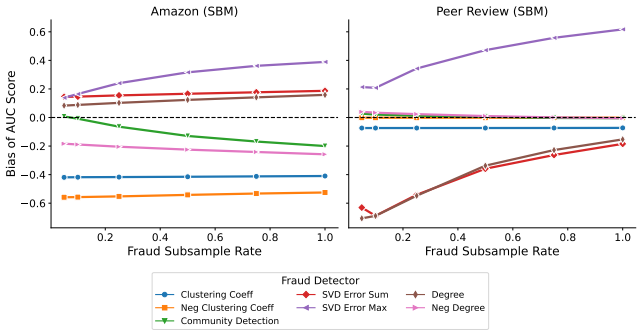


Figure 13: Bias to the AUC score introduced by subsample and aggregate for each fraud detector varying the fraud subsample rate (ρ) while fixing number of partitions $k = 20$.

	# Edges	Degree Sequence	# Triangles	Adjacency Matrix
Yelp	0.45	0.78	1.00	1.50
Elliptic	17.61	25.64	25.13	1.91
Amazon (SBM)	0.99	0.66	0.96	1.00
Peer Review (SBM)	0.21	0.53	1.94	1.66

Table 2: Normalized mean absolute error (MAE) introduced to synthetic graph sufficient statistics at $\varepsilon = 5.0$ and degree cutoff of 0.5 the graph's max degree.

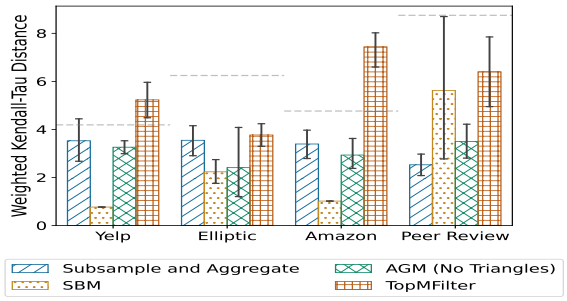


Figure 10: Head-to-head comparison of DP benchmarking methods for $\varepsilon = 5$ overall. Dashed lines show expected Kendall-Tau distance of a random permutation. Error bars show standard errors over 10 trials. SBM and subsample-and-aggregate are the most competitive approaches, though neither uniformly outperforms the other.

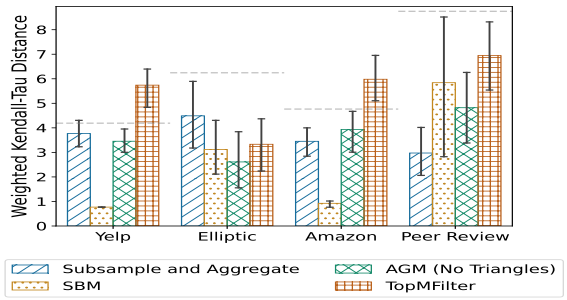


Figure 11: Head-to-head comparison of DP benchmarking methods for $\varepsilon = 2$ overall.

validation is 0.003 and 0.021 respectively reflecting that test and validation sets reliably produce similar leaderboards.

In Figures 10 and 11, we show the Kendall-Tau distance on each dataset for the best choice of parameters with privacy budgets of $\varepsilon = 5.0$ and $\varepsilon = 2.0$ respectively.

B.3 Subsample-and-Aggregate

In this section, we give additional results for subsample and aggregate. First, in Figure 13, we show the bias to different fraud detectors as a function of fraud subsampling rate for the Amazon and Peer Review datasets (as in Figure 3 in the main text.) Then, in Figure 12, we show the bias of each fraud detector as a function of the number of partitions in subsample-and-aggregate.

B.4 Synthetic Data

In this section, we provide additional results for synthetic data methods. In Table 2, we show the error to sufficient statistics using a more aggressive degree truncation threshold of 0.5 times the max degree, compared to 1.0 times the max degree in Figure 4 in the main text. Truncating more aggressively generally increases the error, except on Elliptic, where it decreases the error due to Elliptic being a highly sparse graph.