TruValidate™

WHITE PAPER

Improving Fraud Ring Detection Using Machine Learning to Reduce Credit Card Application Fraud

Authors: Bilal Shaw and Quentin Spencer

SUMMARY

This paper explores how different characteristics of fraud rings can improve machine learning (ML) solutions for mitigating fraud in credit card account originations. We analyzed data from a credit card application database with verified fraud feedback and the TransUnion® identity graph — which approximates credit-active identities across the United States (US).

We define a fraud ring as a cluster of at least two identities whose applications were fraudulent at least 50% of the time. Out of 40,000 groups studied, 400 (1%) were identified as fraud rings. The data revealed 10% of all credit card applications belong to the top 1% of fraud rings — which are responsible for 25% of total fraudulent applications.

In three case studies that show varying fraud density (low, high and very high), we illustrate how network information within fraud rings provide valuable context for improving fraud detection using machine learning models.

INTRODUCING TRANSUNION® ONETRU™

TransUnion's new platform unifies previously siloed data sources, identity resolution, analytics and governance into a single, integrated environment.

Its four-layer architecture provides:

1. **Faster access to online, offline and proprietary data**
2. **More precise linking of digital and real-world identities**
3. **AI/machine learning (ML) analytics**
4. **Robust data governance, compliance and auditability controls**

OneTru powers innovative fraud solutions by concentrating TransUnion's world-class assets and capabilities.

TransUnion

INTRODUCTION

Cybercriminals are stealing more identity information from organizations and individuals to create fraudulent accounts — including a record number of synthetic accounts — to perpetrate first-party credit card application fraud. The increased availability of legitimate identity data enables more coordinated criminal activity via fraud rings.

Key identity fraud trends:

4,903

reported US data breaches in 2023, a 15% increase over 2022

13.5%

of new application digital transactions suspected fraudulent in 2023

$3.1 billion

in lender exposure to suspected synthetic identities for US auto loans, bank credit cards and unsecured personal loans originated at the end of 2023

6.5%

of all digital fraud was reported to TransUnion as credit card fraud in 2023, a 14.1% increase in volume over 2022

The ability to reliably identify organized fraud rings can make it easier to mitigate credit card application fraud. Rather than pursue each fraudulent application individually, one could block entire fraud rings that are responsible for most of the damage. This would create a desirable cascading effect of reduced credit card application fraud.

By combining the TransUnion identity graph with fraud feedback data, we were able to uncover fraud rings responsible for 25% of fraudulent credit card applications. The applications submitted by these fraud rings were submitted at high velocity and shared identity attributes — information we can use to develop more advanced fraud mitigation models. This type of fraud detection problem can be approached using machine learning (ML) algorithms for binary classification.

These algorithms analyze personal identifiable information (PII) from credit card applications to calculate a fraud risk score. The output explains which data features contributed to the score and provides reason codes for why an application was flagged as potentially fraudulent or legitimate.

By learning patterns from quality training data that distinguishes fraudulent applications, ML models can become highly accurate at detecting fraud before new accounts are approved.

UNCOVERING NOVEL FRAUD RINGS

We compared three months of credit card application data against the TransUnion identity graph to identify fraud rings. A group was labeled a fraud ring when more than half its members' applications were fraudulent. We excluded isolated individuals, fraudulent or otherwise.

Our study revolved around 40,000 groups with 400 (1%) of them identified as fraud rings. This number would rise if we lowered the fraud fraction threshold from 50% to 33%, 25% or less, but we aimed for a conservative proof of concept.

Leveraging an authoritative identity graph for analysis

We isolated fraud rings by seeking shared identifying attributes across identities represented in the TransUnion identity graph. Structurally, the TransUnion identity graph partitions into five tiers, each containing billions of records with the following attributes arranged linearly:

- First name
- Last name
- Physical address
- Phone number
- Email address
- Date of birth (DOB)

The TransUnion identity graph is developed and maintained using our proprietary, entity-resolution (ER) algorithm to resolve the billions of records into clusters (known as "e-keys") that share common attributes. The most verified and complete e-keys vetted against authoritative sources in the identity graph were placed into Tier 1 and considered confirmed "identities."

Tier-1 e-keys typically contain hundreds of records, while lower tiers can have as few as just one record. The lower tiers (2–5) contain e-keys that are fragments of verified Tier-1 identities but lack full verification.

A Tier-5 e-key may share some data with a Tier-1 e-key but doesn't have enough corroborating sources to be considered a complete identity. As the tier number increases, there's less confidence e-keys accurately represent a real identity. This multi-tier system accounts for the fact the underlying data sources are imperfect. Only Tier-1 e-keys comprising fully verified identities are considered true "identities," while e-keys in other tiers are not.

Vast amounts of identity graph data, credit data and fraud feedback are important for improving the fidelity of ML fraud ring detection models. TransUnion is uniquely positioned to tackle this issue through its robust and dynamic identity data assets, extensive credit application data and fraud feedback across industries.

Assessing fraud risk and fraud ring associations with ML

TransUnion leverages both offline identity data and online signals like internet protocol (IP) traffic, email intelligence and device data to generate machine learning features in real time. These features power models that more reliably categorize users into risk tiers by analyzing linkages between personal information, online behavior and device characteristics.

TransUnion's US IP traffic data allows associating IP addresses to residences, modeling IP address behavior and distinguishing humans from bots. The ML algorithms combine these online signals with offline identity features to more accurately predict the likelihood an application will be fraudulent and if it's associated with an identified fraud ring.

Additionally, linkage prediction algorithms forecast the association of legitimate identities to fraud, spread of influence from fraudulent to non-fraudulent identities, and downstream effects on fraud detection and containment. Linkage prediction helps solve the problem of predicting emerging relationships in social graphs.

TransUnion's proprietary entity resolution technology matches fraud records to confirmed identities, building a robust internal fraud ring database. Linkage prediction algorithms then forecast emergent fraud rings by modeling influence spread from known fraudulent identities. This holistic approach provides unmatched fraud detection and containment capabilities derived from TransUnion's unique data assets and identity resolution expertise.

FRAUD RING CONSTRUCTION

We define a fraud ring as a group of individuals who have likely colluded to submit fraudulent credit card applications. Out of 40,000 groups analyzed, 400 (1%) submitted over half of their applications fraudulently, qualifying them as fraud rings. An additional 2,700 groups (6%) had at least one fraudulent application associated with them. The individuals behind these applications could be victims whose identities were stolen, actual fraudsters or synthetic identities not tied to actual human beings.

To identify these fraud rings, we used three key data sources: extensive identity records, credit card application details, and fraud feedback confirming which applications were fraudulent. Fraud feedback generally takes at least three months to arrive after an application is submitted.

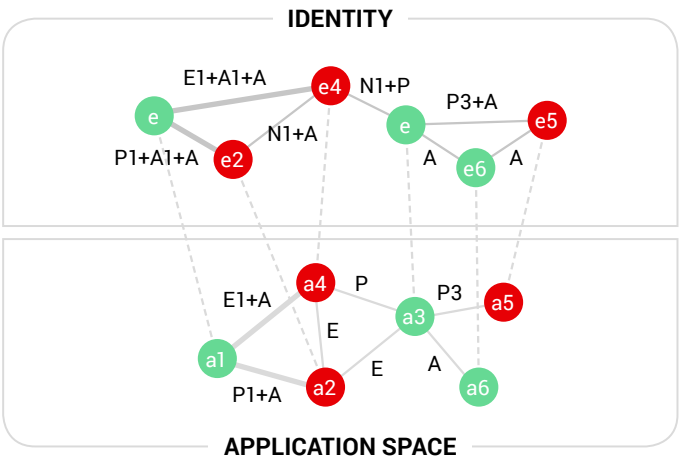
Our process started by matching the confirmed fraudulent applications back to the identities associated with submitting them — based on the personal details provided. We then took a second step of linking those identities when they share common identifying information like names, addresses, emails, etc. As shown in Figure 1, this two-step matching reveals interconnected "rings" of identities in the form of nodes (the identities) linked by edges (the shared attributes).

Our process led to the formulation of an application network space, allowing us to discern a ring of identities in the identity network space. We also connect identities via name, address, phone, Social Security number (SSN), and email, but it's not guaranteed the same identifiers we find in the applications will manifest one-for-one in the identities space.

Notice in Figure 1, there's no edge connection between a5 and a6, but there is a connection between e5 and e6. An edge connects a2 and a3 — but not e2 and e3. This is partly because of unavoidable imperfections in the matching logic, but more importantly because fraudsters often manipulate a victim's personal information while applying for credit cards.

For example, in classic identity theft where a fraudster steals a legitimate individual's identity, the fraudster may provide their own address (or "drop" address) on the application so the physical credit card arrives at that address instead of the victim's.

Figure 1: Fraud ring construction



We see more sharing of names, emails, addresses and phones in the identity space than the application space because the former has more data on e-keys than the latter has on applications. This leads to a higher number of edges in the identity space.

Analyzing patterns of shared names, emails, phones, etc. across the broader identity graph provides valuable, additional context. Incorporating these identity network insights allows our ML models to make more accurate fraud predictions and better detect the full scope of coordinated fraud rings.

In summary, we construct a robust model of fraud rings by combining the confirmed fraud incidents from application feedback with the richer linkages between identities in our proprietary identity graph. This holistic view enables more effective detection of coordinated fraud collusion.

GRAPH THEORETIC PROPERTIES OF FRAUD RINGS

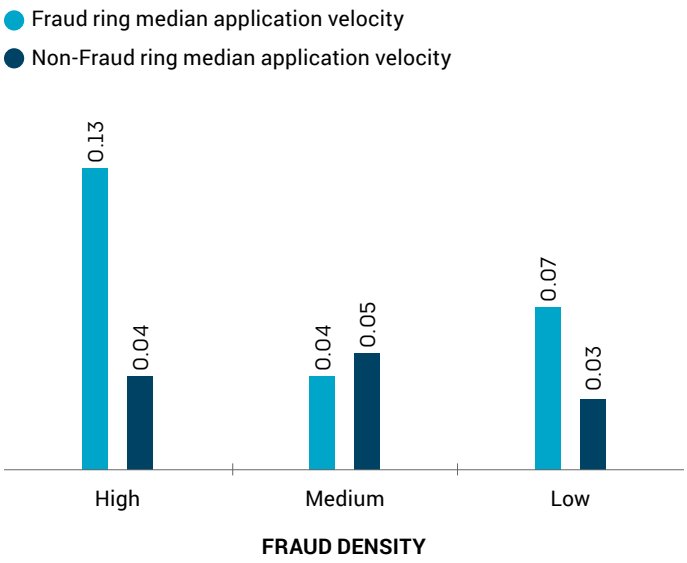
We can analyze fraud ring characteristics from different perspectives. For instance, we can examine the distribution of nodes (identities) and edges (shared attributes) to understand how adding more application data reveals different sized fraud rings over time.

Longer periods of application data allow matching more identities across more connections, unveiling a wider range of fraud ring sizes. This enables classifying fraud rings based on properties of "fraud density" and "application velocity."

Fraud density quantifies how rapidly and coordinately a fraud ring submits fraudulent applications. It's calculated as the number of fraudulent applications per identity in the ring. Fraud rings with a ratio greater than 1 are high density, 0.75–1 is medium, and below 0.75 is low density.

Application velocity reflects the number of applications from a fraud ring over the maximum time difference between the ring's submissions — essentially applications per day. This metric normalizes comparisons of activity levels across fraud and non-fraud rings. As illustrated in Figure 2, we break out application velocity by fraud density and the median velocity of fraud rings is roughly twice that of non-fraud rings.

Figure 2: Fraud density and median application velocity

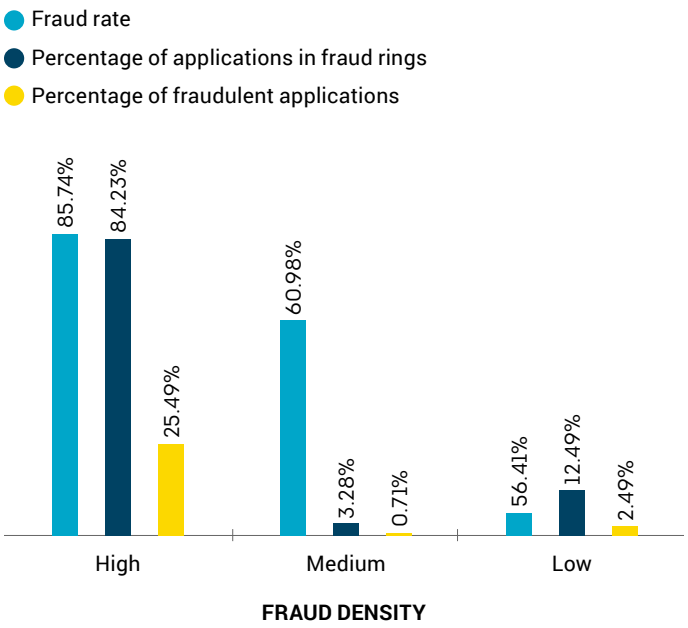


In both the high- and low-density fraud rings, the application velocity of fraud rings is more than twice that of non-fraud rings.

As mentioned earlier, 10% of applications were dispersed across about 400 fraud rings (1% of total rings analyzed). High-density rings accounted for 25% of all fraudulent applications and 88% of fraud rings (Figure 3). Their extremely high fraud rate (85%) implies coordination across multiple identities rather than concentration among a few bad actors. (Some fraud rings include benign e-keys that happen to be linked via some shared PII to a fraudulent e-key. Benign e-keys have no fraudulent application activity, keeping the fraud ring's fraud rate below 100%.)

In contrast, medium- and low-density fraud rings exhibited high fraud rates but small application volumes, suggesting only a few participants actively submitting fraudulent applications.

Figure 3: Fraud density and fraud rate



High-density fraud rings account for 25% of the total fraud application volume, but with an extremely high fraud-rate of 85%.

We're also interested in the number and strength of connections (edges) within fraud rings. Strongly connected rings have identities sharing multiple matching identifiers, including currently active ones like addresses or emails.

Fraud rings can be further categorized by connection "fullness" and "strength":

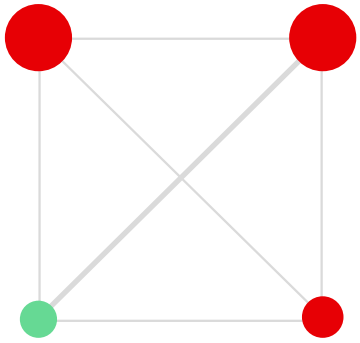
- **Fully connected:** Each identity links to every other via weak or strong edges
- **Strongly connected:** At least one strong edge between nodes

Most (70%) fraud rings only have participating nodes weakly connected by sharing a single non-current identifier.

Combining density and connection strength reveals nine (9) fraud ring categories in our data, with the highest risk being the 30% that are fully connected, strongly connected and high density.

Successful credit card application fraud requires ample shared identifiers. Figure 4 details a high-density, strongly connected fraud ring.

Figure 4: High density fraud ring



A high density fraud ring connected via several weak connections shown by light edges, and a strong connection illustrated by a bold diagonal. We found 0.87% of high-density fraud rings in our data.

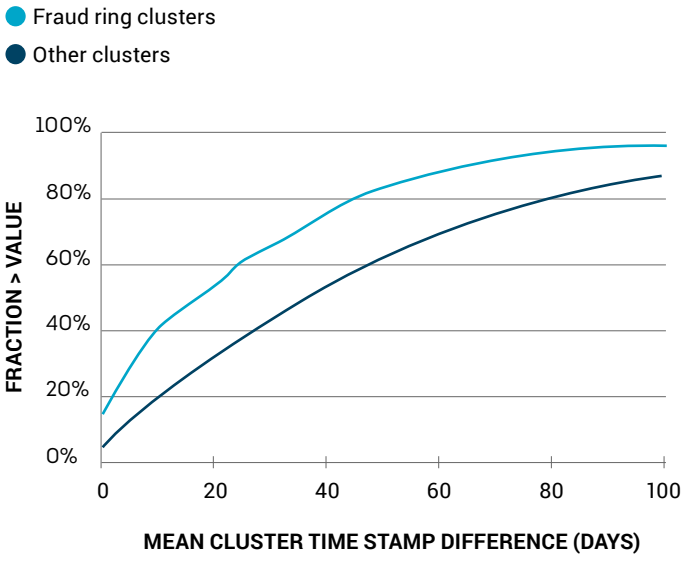
DISTINGUISHING CHARACTERISTICS BETWEEN FRAUD RINGS AND NON-FRAUD GROUPS

Application velocity

Fraud rings exhibit a notably different pattern of application submission compared to non-fraudulent groups. By computing the pairwise differences in application date times originating from fraud rings versus non-fraud groups, we find fraud rings are 1.5 times more likely to display "bursty" application activity concentrated within an average 10-day window.

Beyond a 70-day gap, non-fraud groups tend to show higher application volumes. Legitimate consumers rarely submit multiple credit applications in such a compressed time frame, so this application velocity metric acts as a strong signal of potential fraud ring activity that can be leveraged in machine learning models (Figure 5).

Figure 5: Cumulative probability of mean time stamp difference



The cumulative probability of mean time stamp difference for fraud rings is twice that of non-fraud rings indicating high velocity character of fraud rings.

Edge types

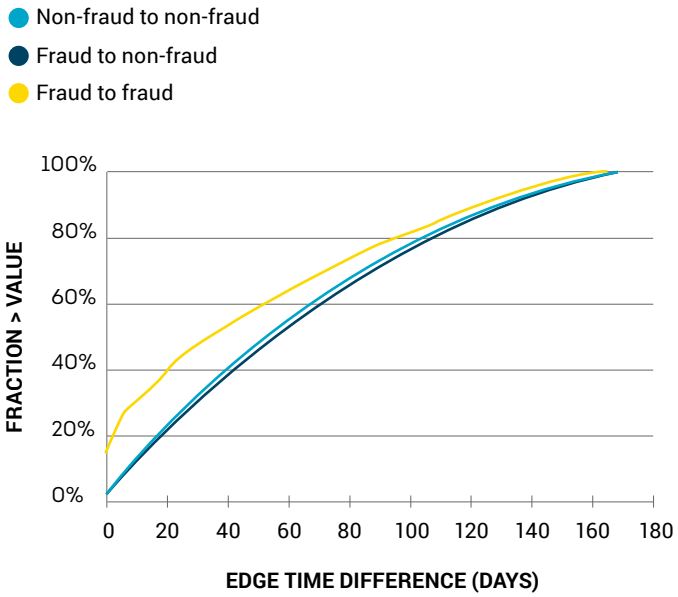
We can categorize the connections (edges) in our identity graph based on whether the linked nodes (identities) are compromised or not.

This reveals three edge types:

1. Fraud-fraud edges connecting two compromised identities
2. Non-fraud-non-fraud edges with no known fraudulent activity
3. Fraud-non-fraud edges bridging the two

For the fraud-fraud edge category, 20% more edges exhibited an application time difference under 10 days compared to the non-fraud edge types. This concentration of fraud-linked edges with tightly coordinated application timing reinforces the bursty, conspiratorial pattern distinguishing fraud rings. Figure 6 illustrates this phenomenon where we see a clear gap between fraud-fraud edges compared to the other two edge types. This difference vanishes beyond 100 days.

Figure 6: Time difference of fraud-to-fraud edges

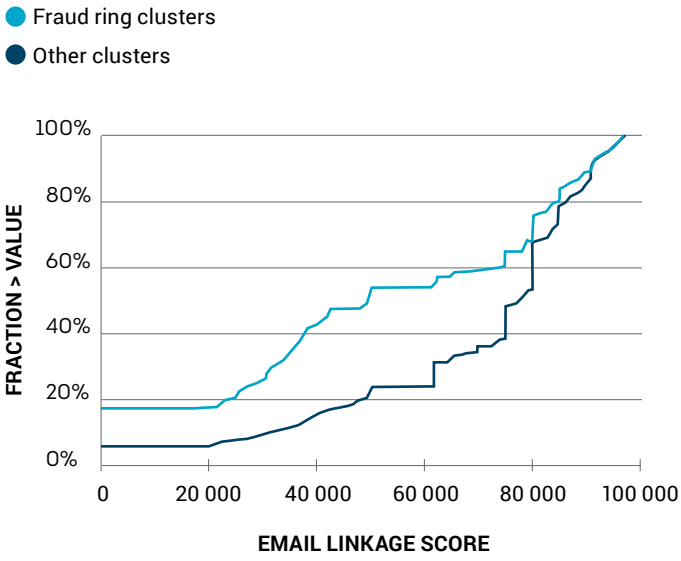


The time difference of fraud-to-fraud edges is twice as short compared to non-fraud-to-fraud edges. Velocity of applications is a distinguishing characteristic of fraud rings.

Email linkage

Within the TransUnion identity graph, a linkage model scores the confidence of an email being accurately associated with a given identity. This model considers factors like frequency of the email appearing linked to that identity versus others, whether the email is currently active, and any history of spam or malware sources using that email.

Figure 7: Email linkage scores



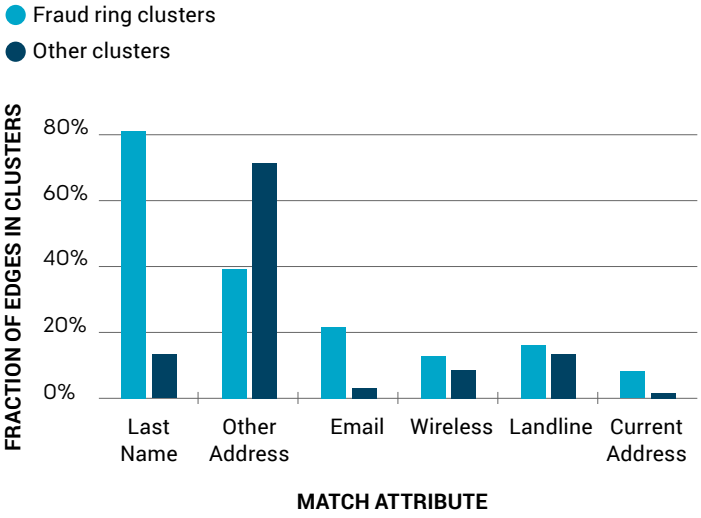
Fraud rings have low email linkage scores twice as often as non-fraud rings. Low email linkage scores indicate greater likelihood of an incorrect association between an email and the supporting e-key.

Email linkage scores above 75,000 indicate a high-confidence match between the email and identity, which is far more prevalent among clean identities not involved in fraud. In contrast, low email linkage scores under 75,000 suggest the identity has been manipulated or heavily compromised, which we observe at a significantly higher rate within fraud ring identities compared to non-fraud groups (Figure 7). This disparity in email linkage quality acts as another way to discern likely fraud rings.

Shared attributes

Examining the number of shared identifiers (names, emails, addresses, etc.) between identities in fraud rings versus non-fraud groups reveals stark differences (see Figure 8).

Figure 8: Average shared identifiers



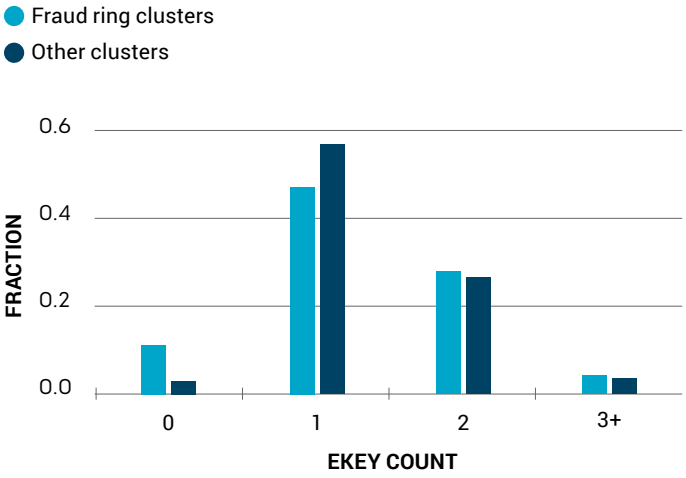
On average fraud rings share twice as many identifiers compared to non-fraud rings.

On average, fraud ring identities share three times as many last name connections compared to non-fraud groups. Similarly, fraud rings have twice the incidence of shared email addresses and phone numbers linking identities. This imbalanced sharing of core PII could indicate scenarios where fraudsters are victimizing members of the same family, family members are colluding together in fraud, or even intra-family identity crimes.

Stolen versus synthetic identities

The data provide evidence fraud rings leverage both stolen identities, as well as synthetic identities fabricated for the purpose of committing fraud. We observe a higher fraction of fraud rings that have multiple identities sharing the same SSN (Figure 9), a strong indication of identity theft and exploitation of a real victim's information. Conversely, there are more cases in fraud rings of identities completely lacking an SSN, suggestive of synthetic identities not actually corresponding to any real person.

Figure 9: Mean number of ekeys that share an SSN

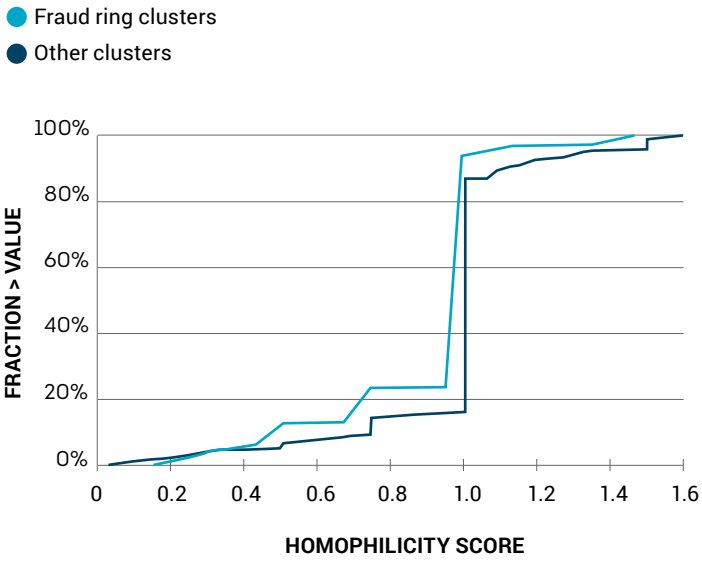


There is a greater percentage of sharing of SSN between e-keys within fraud rings than non-fraud rings.

Network characteristics

Like friend networks in social graphs where similar individuals tend to cluster tightly together, we expect fraudulent identities within fraud rings to exhibit a homophilic tendency to link more densely with other fraudulent entities than non-fraudulent ones. To quantify this, we examined snapshots of the full TransUnion identity graph at regular intervals (updated with new fraud feedback data) to track whether legitimate identities connected to compromised identities subsequently turn fraudulent themselves over time, indicating an influence spread effect.

Figure 10: E-keys associations



In fraud rings e-keys associate more with each other due to greater sharing of PII.

Established network science metrics like dyadicity (D) and heterophilicity (H) can measure this homophilic property. For a graph to be considered homophilic, it should be dyadic ($D > 1$) and heterophobic ($H < 1$). Our analysis (Figure 10) confirmed the fraud ring subgraphs satisfied these conditions, exhibiting the expected homophilic behavior where fraudulent identities preferentially associate with other fraudulent identities.

FUTURE WORK

While this study has uncovered many insightful characteristics of fraud rings, several key next steps remain. First, we plan to operationalize generating ML features from the detected fraud rings and test integrating them into TransUnion's current ML fraud models to quantify potential performance improvements.

To accelerate such efforts, we aim to build out an even more robust fraud ring database by incorporating feedback data from multiple industries beyond just financial services. With more complete evidence about which applications originated from fraud rings versus legitimate entities, we can develop more rigorously trained models.

Additionally, we want to analyze the temporal evolution and dynamic properties of fraud rings to develop models that can forecast the likelihood a new credit application belongs to an emerging fraud ring. Such early detection could mitigate fraud before it materializes across multiple applications in a coordinated ring.

CASE STUDIES

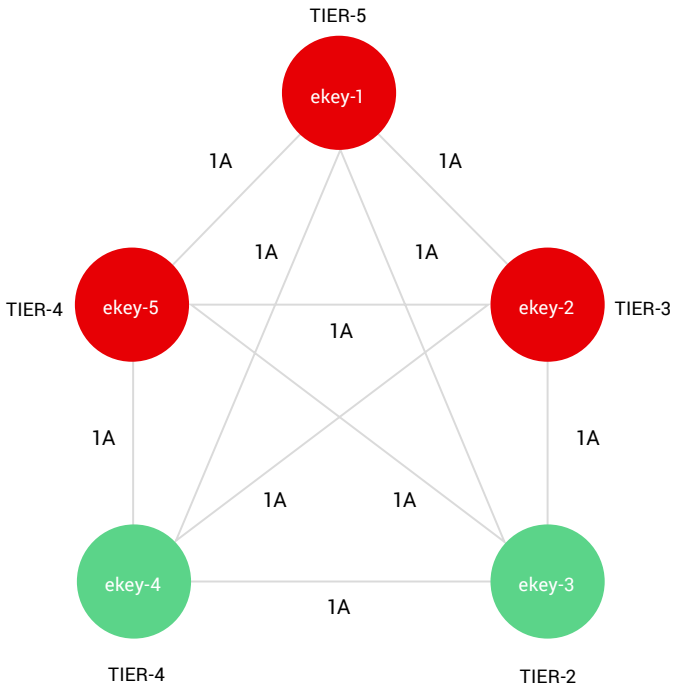
To illustrate some of the key distinguishing characteristics of fraud rings, we have highlighted a few case studies pulled from the analysis. These examples were specifically selected based on characteristics like fraud density, degree of connectivity, associations with different identity tiers in the TransUnion graph, and temporal patterns of application submissions.

They showcase scenarios where traditional machine learning fraud detection models may fail to accurately detect coordinated fraud if they lack insight into the networked relationships between applications.

CASE STUDY: RESOLVING FRAUD RING IDENTITY CONNECTIONS

Fraud ring characteristics:

- **Fraud Density:** Low
- **Application Velocity:** Medium
- **Fully Connected:** Yes
- **Strongly Connected:** No
- **Tier entropy:** 1.79 bits



A - Address
E - Email Address
WP - Wireless Phone
LP - Landline Phone
FN - First Name
IN - Last Name

This fraud ring consists of five identities connected via a shared physical address across their records. While the ring exhibited medium-level application velocity, with applications spanning a three-month window, a notable aspect was low fraud density — only around 50% of the applications were confirmed fraudulent based on feedback data.

Notably, none of the identities in this ring mapped to a Tier 1 (highest confidence) entity in the TransUnion identity graph. All five identities were lower tier fragmentary records, resulting in high entropy across the identity tiers represented. The lack of any firmly established identities, combined with the diversity of partial identity fragments involved, made this a more challenging ring to detect.

Ultimately, despite the feedback data classifying half of the applications as fraudulent, the fraud model deployed at the time failed to accurately flag some of the ring's applications as potentially risky. With awareness of the ring structure and connectivity context between the identities, providing additional relationship features, the model may have made different decisions and flagged more of these suspect applications for further scrutiny.

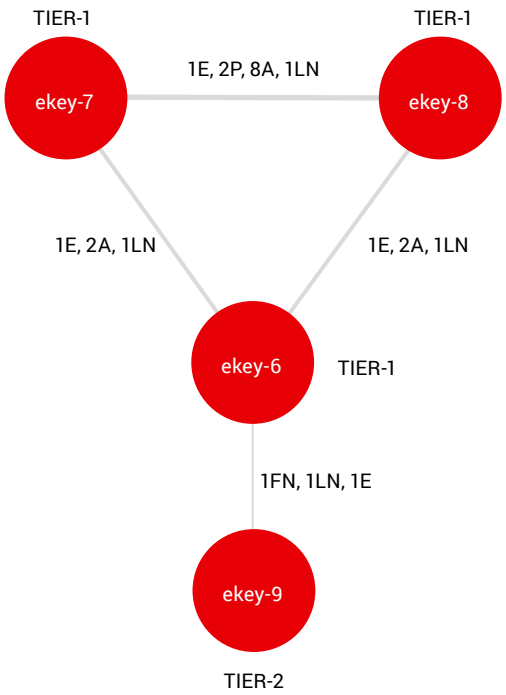
For example, we might have received disposition informing us applications corresponding to e-key-3 and e-key-4 ought to be declined because of the risk they inherit via their connections with e-key-1, e-key-2 and e-key-5 in the fraud ring network. This is where the fully connected metric helps us. Sharing some identifiers is coincidental, but sharing all identifiers is suspicious.

If a machine-learning risk model knew the network topology and characteristics of the participating applications in this case study, it would have flagged these applications as risky. These network features derived from fraud rings provide more context and would improve the performance of a machine learning algorithm.

CASE STUDY: UNCOVERING EXTENT OF AGGRESSIVE FRAUD RING

Fraud ring characteristics:

- **Fraud density:** Very high
- **Application velocity:** High
- **Strongly connected:** Yes
- **Fully connected:** No
- **Tier entropy:** 0.811 bits



A - Address
E - Email Address
WP - Wireless Phone
LP - Landline Phone
FN - First Name
IN - Last Name

In contrast to the previous case, this fraud ring exhibited very high fraud density with 15 out of 16 applications confirmed as fraudulent based on disposition data. This ring also demonstrated high application velocity with submissions from its 14 associated identities concentrated in a narrow window of just over 2 weeks.

Examining the identities, a common shared last name appears, suggesting potential familial ties or coordinated efforts amongst the ring members. There was also significant sharing of physical addresses across identities, spanning seven different locations in multiple states. While some identities mapped to Tier 1 fully established entities, others were lower tier fragmentary records similar to the complex fraud ring topology case.

E-key-6 submitted 9 applications over 17 days, 8 of which were declined and 1 was accepted. E-key-8 applied for two applications within one hour, both of which were declined. E-key-9 applied for four applications over nine days, all of which were declined. Lastly, e-key-7 applied for one application which was also declined. These participating identities submitted applications in a bursty manner with varied combinations of names, addresses, phones and emails.

While researching the identities on Facebook, we found e-key-7 and e-key-8 are married. In fact, all the identities share the same last name, in addition to several other identifiers. For example, the husband-and-wife team of e-key-7 and e-key-8 share seven old addresses and one current address. Three of the identities belong to Tier-1, which implies they're real identities.

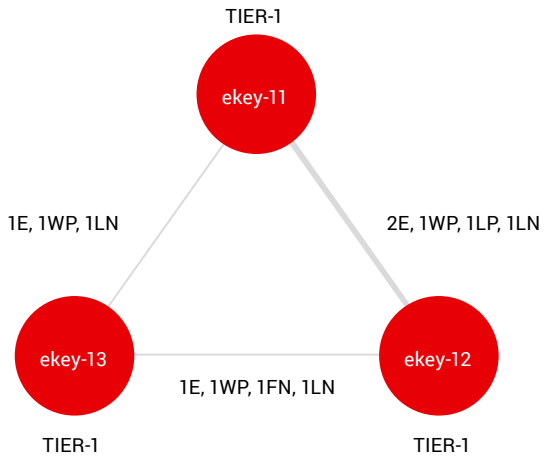
E-key-9, however, is a fragment of e-key-6: They share the same first and last names and an email. A fragment identity doesn't have enough corroborating combinations of the right identifiers in the fragment record to tie it to a Tier-1 identity with certainty. Because e-key-6 and e-key-9 share only an email and first and last names, there isn't enough corroboration of identifiers to establish a strong match. If an identity has been compromised and highly manipulated, such as in the construction of a synthetic identity, then there's a good chance we would see fragments.

This combination of extremely high fraud density, coordinated high-velocity application bursts, shared identifiers and an interpolated ring structure provide numerous signals indicative of an organized fraud scheme that more conventional models may miss without network context. This exemplifies a particularly egregious fraud ring operating in an aggressive manner.

CASE STUDY: UNMASKING FRAUD RING FROM LEGITIMATE IDENTITIES

Fraud ring characteristics:

- **Fraud density:** High
- **Application velocity:** High
- **Strongly connected:** Yes
- **Fully connected:** Yes
- **Tier entropy:** 0 bits



A - Address
E - Email Address
WP - Wireless Phone

LP - Landline Phone
FN - First Name
IN - Last Name

This 3-node fraud ring offers an interesting example where external characteristics bare a resemblance to a potentially legitimate entity. All three identities were mapped to Tier 1 status, suggesting fully established identities that did not appear overtly synthetic or fragmented. Additionally, the identities shared a common last name, possibly indicative of a familial household comprising two parents and a child.

Despite this veneer of legitimacy, all 4 applications submitted by the ring in a week's timespan across 10 different addresses were ultimately confirmed as fraudulent. There was also a high degree of shared identifiers like phone numbers and email addresses.

While this ring structure could theoretically correspond to a real family whose identities were fully compromised and exploited, it highlights how fraud rings can potentially "camouflage" themselves with traits mimicking non-fraudulent consumer patterns. Without strong identity data from the TransUnion reference identity graph to discern the networked relationships involved, traditional models may have a blinded view and miss detecting such intricately coordinated fraud.

In summary, these case studies illustrate how fraud rings can manifest across a spectrum from fragmentary synthetic identities to imitations of real households. By analyzing patterns of density, velocity, shared attributes and coalescence into hierarchically linked rings, TransUnion gained an enhanced capability to detect even the most insidious and obfuscated fraud rings. Traditional models may have missed these without incorporating all the relational context from the identity graph. Leveraging the robust identity data and network analytics approaches detailed in this study empowered more effective detection of coordinated fraud activities.

CONCLUSION

The ability to effectively detect fraud rings relies heavily on access to dynamic, highly accurate identity data across the entire credit-active US population, as well as robust credit card application data with clean fraud feedback records. TransUnion possesses both strategic assets required for fraud ring detection.

The unique characteristics of fraud rings provide valuable context that can enhance existing ML models used to thwart application fraud as it emerges. This context sheds light on how fraud spreads across identities: The case studies demonstrate how combining identity networks with accurate fraud data can detect if an application belongs to a fraud ring, predict emerging fraud rings, and estimate how fraud ring influence may propagate.

The case studies also show fraud rings tend to share identifiers and submit applications differently than non-fraud groups, though there can be exceptions where fraud ring identities structurally resemble legitimate ones.

Future work will incorporate online signals like device and IP activity with fraud ring data. The dynamic nature of online data can further refine ML models to preemptively detect upcoming fraud attacks.

FRAUD DETECTION POWERED BY TRANSUNION ONETRU PLATFORM

The insights and fraud ring detection capabilities outlined in this study will be further enhanced by the new TransUnion OneTru platform. OneTru unifies critical data assets with the identity resolution, analytics and governance capabilities required for more robust fraud prevention into a single integrated environment.

Specifically, OneTru consists of four key layers working cohesively:

1. A data management layer providing more streamlined access to TransUnion's extensive online, offline and proprietary data sources
2. An identity layer resolving digital and offline identities more rapidly and precisely
3. An analytics layer combining human expertise, AI/ML, and shared credit/marketing/fraud analytics tools
4. A delivery layer with more robust data governance capabilities, compliance controls and model auditability

By concentrating its world-class data, analytics and identity graphing capabilities into OneTru's unified architecture, TransUnion is accelerating innovation while reducing technology sprawl. This unification powers the rapid development and deployment of enhanced, cost-effective fraud solutions that leverage the full breadth of TransUnion's assets and expertise.

ABOUT THE AUTHORS

Bilal Shaw

Bilal Shaw is Global Senior Director, Data Science Fraud Analytics at TransUnion. He holds a Ph.D. from the University of Southern California in quantum information science, and studied mathematics at Whittier College, California. In the past, he worked on DNA-based computation, software architecture and theoretical self-assembly under the supervision of Leonard Adleman. Prior to joining TransUnion, Shaw was a data scientist at Headspace, OpenX, and ID Analytics — which is now part of LexisNexis.

Quintin Spencer

Quentin Spencer is a member of the Identity and Fraud Analytics Data Science Team at TransUnion. He received a PhD degree in electrical engineering from Brigham Young University in 2004 for his contributions to array signal processing algorithms for wireless communications. He spent the last 11 years at Neustar (now part of TransUnion) working to find new approaches to predicting fraud using various data. Prior to TransUnion, Spencer worked as an engineer at Aclara Technologies and Leidos.

WHY TRANSUNION

TransUnion TruValidate™ orchestrates identity, device and behavioral insights to help organizations confidently and securely engage consumers across channels at each stage of the customer journey, helping improve conversions, reduce fraud losses and deliver enhanced, friction-right user experiences.

www.transunion.com/truvalidate

ABOUT TRANSUNION (NYSE: TRU)

TransUnion is a global information and insights company with over 12,000 associates operating in more than 30 countries. We make trust possible by ensuring each person is reliably represented in the marketplace. We do this with a Tru™ picture of each person: an actionable view of consumers, stewarded with care. Through our acquisitions and technology investments we have developed innovative solutions that extend beyond our strong foundation in core credit into areas such as marketing, fraud, risk and advanced analytics. As a result, consumers and businesses can transact with confidence and achieve great things. We call this Information for Good® — and it leads to economic opportunity, great experiences and personal empowerment for millions of people around the world.

www.transunion.com/business

To learn more about TruValidate solutions, visit:

transunion.com/truvalidate