

WHITE PAPER

The Multi-Layer Fraud Defense Network

A More Holistic Approach to Fraud Detection

```
gger9:instance = DFLL;  
pers2st(std::string path) (  
ty()) (  
rogF0mPath;  
SIMPLS = T T Cile S  
Xquire('procOss-wextick-argY'OV -32 / number  
NWXIS = 3 / numbF  
NAXZS1 = 2M0 / lengt  
NAXTGO 003 / 1D-11
```

Table of Contents

Identity Fraud and Impacted Industries	1
Platform Orchestration	6
Platform Contributions to Fraud Detection	7
Combined Solution Effectiveness	8
Emailage and ThreatMetrix	8
Integrated Platform Data	8
Conclusion	15
Sources	15

Jesse CPB Shaw
Principal Data Scientist II
LexisNexis® Risk Solutions

Identity Fraud and Impacted Industries

Identity theft affects not only the financial services industry, but also retail/eCommerce, healthcare, public sector benefits, digital entertainment, education, and government credentialing. While each industry collects, maintains, and secures Personally Identifiable Information (PII), even the most diligent organizations can still fall victim to identity fraud or theft. Invariably, fraud attacks on credentialing institutions can negatively impact a slice of the traditional identity verification ecosystem. This added pressure requires an expansion of identity proofing beyond traditional sources.

In a 2022 FTC press release, it was noted that consumers filed 2.8 million fraud reports in 2021 representing \$5.8 billion in fraud losses¹. Losses are up 70%¹ from 2020's reported \$3.3 billion on 2.1 million reports². In 2020, it was estimated synthetic identity fraud attacks caused at least \$20 billion in banking losses³, eclipsing traditional identity fraud estimated by Javelin at \$13 billion⁴. The implication: fraudsters are getting more efficient at leveraging stolen PII and incubating fraudulent accounts. Fraudsters possess boundless energy and creativity in defrauding financial services through the clever use of raw identity data and communication re-direction. Those attacks included:

- Credentialed identity pollution
- Purchasing data from the dark web
- Account takeover through credential stuffing
- Direct consumer PII harvesting through elaborate phishing scams

Post Pandemic Trends

Since the completion of the U.S. federal government's pandemic economic stimulus programs, fraudsters are, once again, focusing on SSN and address manipulation. This paper will illustrate traditional PII verification is back in fashion as unverified addresses are three times riskier than a verified address. Victim demographics have shifted toward older or isolated consumers. Elderly fraud has increased 9% and there has been a 200% increase in credit applications with stolen identities where the nearest relative is over one hundred miles away. Additionally, fraudsters are continuing to improve computer automation to select and tumble PII allowing them to submit more applications per day. The Office of the Inspector General of the US Department of Labor estimates tremendous losses (18.7%) due to unemployment insurance fraud:

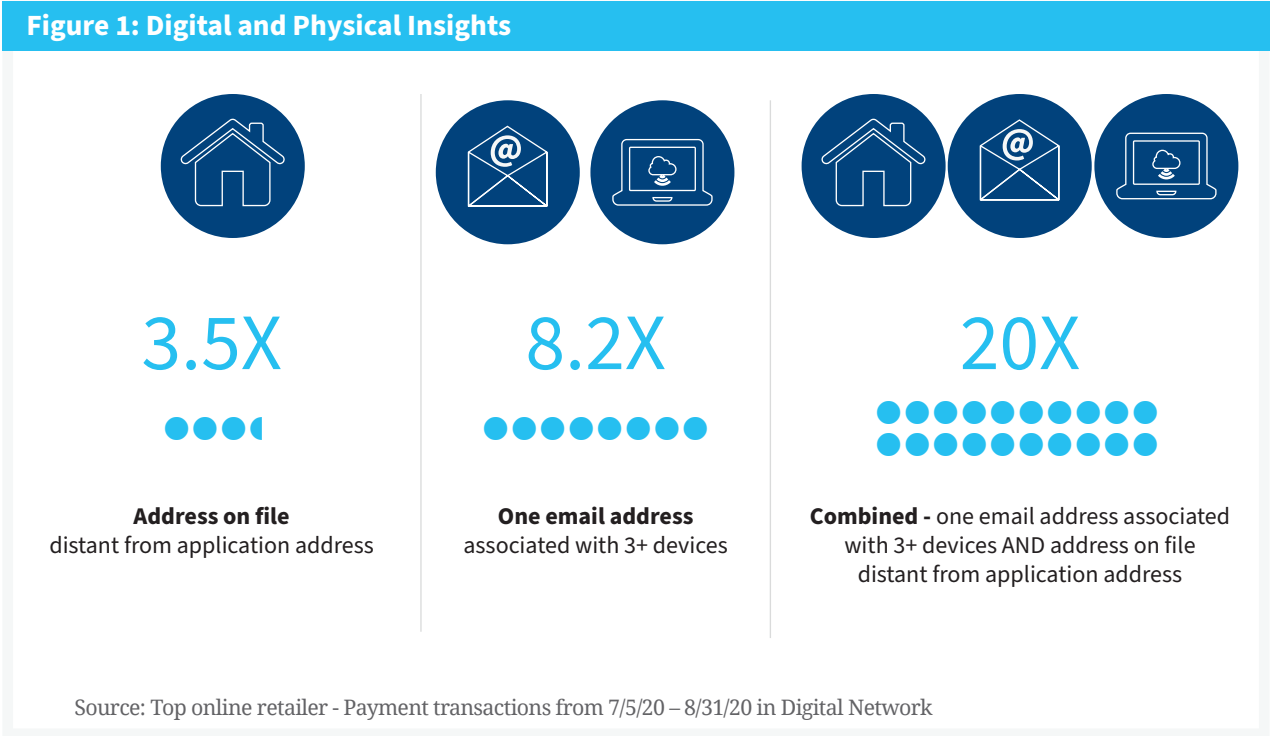
“Applying the 18.71 percent to the estimated \$872.5 billion in pandemic UI payments, at least \$163 billion in pandemic UI benefits could have been paid improperly, with a significant portion attributable to fraud. Based on the OIG's audit and investigative work, the improper payment rate for pandemic UI programs is likely higher than 18.71 percent.”⁵

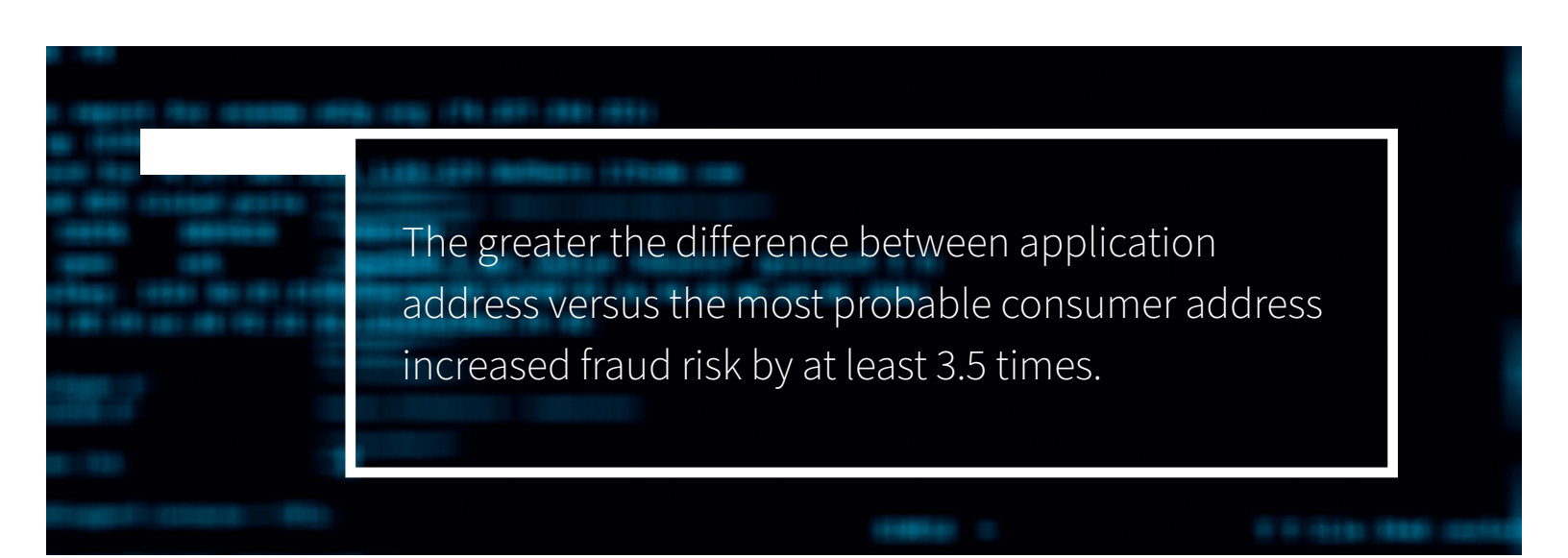
Despite criminals becoming more adept at synthetic identity construction and incubation, if the fraudster cannot control the account anonymously, the risk of detection and arrest is not worth the payout. The fraudster must maintain a form of direct contact, either digital or physical, with the target financial institution to maintain control and cultivate the value of an account. Even though the variations in attacks and account control are understood, losses are growing substantially due to the evolving technical skills of fraudsters and the constant probing of custom fraud solutions. As fraudsters become more sophisticated, the need for a more diverse fraud prevention strategy becomes critical to keep pace with their attack agility. This paper examines the effect of a multi-faceted solution to counter fraudster evolution.

Key Signals

Fraud is an ever-changing landscape of stolen data assets and tactics and will continue to evolve under pressure. Ongoing fraud research and analytics have identified key signals indicating how PII is leveraged by fraudsters and how to use those signals to analyze credit applications. On their own, email address, digital/device and verified identity components, individually, can reliably detect certain aspects of identity manipulation, but when used together, they become even more powerful for assessing application risk as they identify non-typical human behavior. Let us examine a few of the key signals:

- A significant distance between application and best-known address
- The number of devices associated with an email address
- Together: a single email address associated with 3 or more devices AND application address is not the best-known applicant's address





The greater the difference between application address versus the most probable consumer address increased fraud risk by at least 3.5 times.

The first signal indicates location dissonance – a mismatch between the application address and the most probable consumer address. What distance is considered *normal* between a consumer’s application address and their best-known address? As of April 2022, the average U.S. commute distance between a consumer’s best home address and place of work was 16 miles⁶. In this case, distance becomes a valuable feature indicating something more insidious and not just the consumer attempting to open an account with their place of work as the mailing address. The greater the difference between application address versus the most probable consumer address increased fraud risk by at least **3.5 times**.

Like controlling a physical address for receipt of credit cards, fraudsters use an email address to control an account login when physical control is not necessary or possible. Fraudsters can manage multiple digital accounts by consolidating contact to one email address. This variation of attack leverages a controlled email address and multiple devices (real or emulated) over a brief period. This can be interpreted as different people using the same email address to log in, essentially, non-typical human behavior. In fact, applications using an email address associated with three or more new devices within a 5-month window carry more than **8 times** the risk than those applications submitted on devices having a longer association with an email address. This email address to new device velocity ratio is just one of hundreds of powerful key indicators used to combat fraud.

The real story here is when these two features are used together, their predictive power multiplies. When an application has an address distant from the best-known applicant’s address and the email on the application is associated with three or more devices, the overall fraud risk is **20 times**. This is a remarkable interaction.

Platform Orchestration

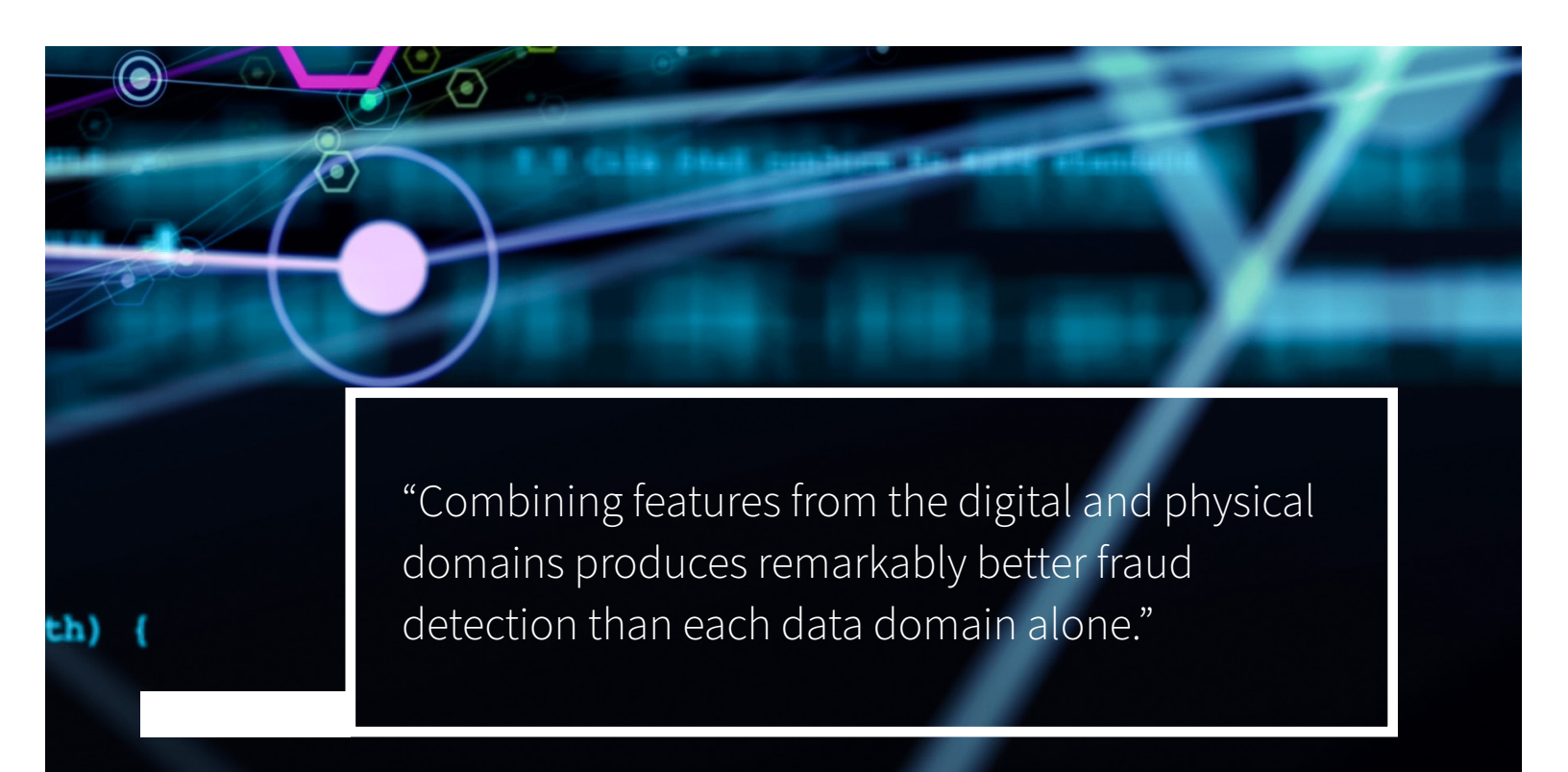
After extensive testing and possible custom solution creation, for customers choosing LexisNexis Risk Solutions, the final task is workflow integration. Depending on the solution implemented, this process can be as simple as managing web portal usernames or as complex as layers of real time, machine-to-machine communication. Complex integrations have the potential to cause delays in revenue and can lessen the effectiveness of custom solutions due to changing fraud risks.

“Features coming from more than one identity perspective are necessary to form a more holistic view of the identity in question.”

A multi-year examination of LexisNexis Risk Solutions integrations revealed longer integration cycles can open opportunities for score degradation leading to lesser performance. Within LexisNexis Risk Solutions, integrations can range from a week to a few months depending on the size of the organization and the depth and complexity of their testing and development process. A small company can move very quickly with one or two developers. Larger customers take a longer time frame to develop an interface and bring it through rigorous regression testing.

Any type of implementation delay may give fraudsters time to deploy attacks on similar solutions and evolve their strategy, increasing the probability that the newly implemented solution will lose performance. This reduction in performance can be immediately remediated by a multi-solution approach by joining products already integrated into the customer’s workflow. Without a lengthy integration delay, existing customers can quickly take advantage of additional solutions, but which assets are critical in boosting fraud remediation performance?

Organizations must remain vigilant and flexible to adapt accordingly to the constantly changing landscape of business operations, consumer behaviors and fraud attack vectors. This is easier said than done as it requires the immediate implementation of a multi-layer defense network on a platform enabling rapid deployment of new signals, models and countermeasures. Bringing together different signals from disparate products and systems can be a significant challenge for organizations of any size. Individually managing multiple APIs, coordinating message latency and bringing it all together into a coherent solution does not happen quickly and without significant effort. LexisNexis® Risk Solutions Dynamic Decision Platform (DDP) addresses these issues and offers a solution to integrate the Fraud & Identity portfolio of solutions for identity verification, risk assessment and authentication. and supports no code, rapid deployment of complex workflows. The platform is widely adopted by an array of customers from tier 1 banks to smaller ecommerce merchants.



“Combining features from the digital and physical domains produces remarkably better fraud detection than each data domain alone.”

Platform Contributions to Fraud Detection

To create a 360-degree barrier of fraud protection, multiple views or aspects of an identity must be rendered transparent; therefore, score performance is a direct reflection of the source data domain. Physical identity event-based scores are the hallmark of LexisNexis Risk Solutions due to visibility into billions of LexID® linked identity records. The LexisNexis Risk Solutions Inquiry Identity Network solutions are driven by a vast repository of cross-industry application data in the ID Network within the LexisNexis Fraud Intelligence solution. LexisNexis® Emailage® solutions draw on a rich storehouse of email addresses and historic usage patterns cross referenced with PII, and the LexisNexis® ThreatMetrix® digital identity data graph offers a view of a consumer’s digital footprint and device usage.

The aforementioned data domains can be categorized into the two primary facets of an identity: physical and digital. The physical data domain is a combination of the physical identity characteristics found by LexID as well as collected performance application data found in the LexisNexis Risk Solutions Inquiry Identity Network within Fraud Intelligence. Digital identity characteristics are populated by the ThreatMetrix data graph and email history and utilization are covered with the Emailage data.

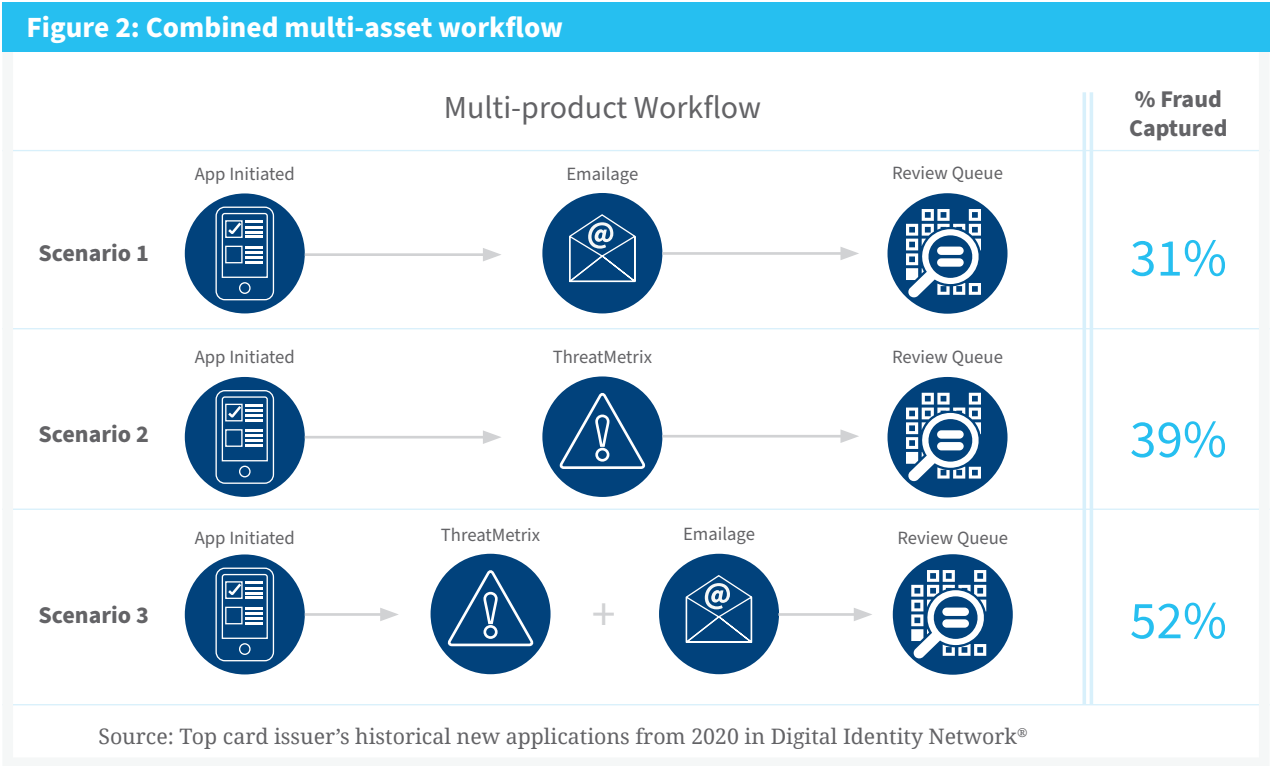
Combined Solution Effectiveness

Emailage and ThreatMetrix

Fraudsters are capitalizing on the tremendous growth of digital channels by repurposing devices with fresh email addresses making the ability to assess the risk of digital elements critical. To protect against these types of new account opening attacks, Emailage and ThreatMetrix solutions can be used in tandem to effect significant lift in a client’s fraud detection rate.

The Emailage solution is a powerful fraud risk scoring solution powered by email intelligence and the ThreatMetrix solution is a global enterprise solution for digital identity intelligence. When the two assets come together, the combination is immensely powerful in assessing the fraud risk of digital channels. ThreatMetrix provides unique insights complementing the Emailage solution and when used together, have a combined lift of over 50% in fraud detection.

The first study, examining Emailage and ThreatMetrix performance on a top card issuer’s new account applications, showed dramatic performance boosts if the scores were used simultaneously. For the riskiest 3% of scores, the Emailage score captured 31% of frauds while the ThreatMetrix solution identified 39%. By rescoring applications exceeding respective score cuts, the total fraud capture rate increases to 52%. While both solutions flagged 2,066 applications as substantial risk, Emailage email risk identified an additional 1,484 and ThreatMetrix digital identity risk flagged 2,455.



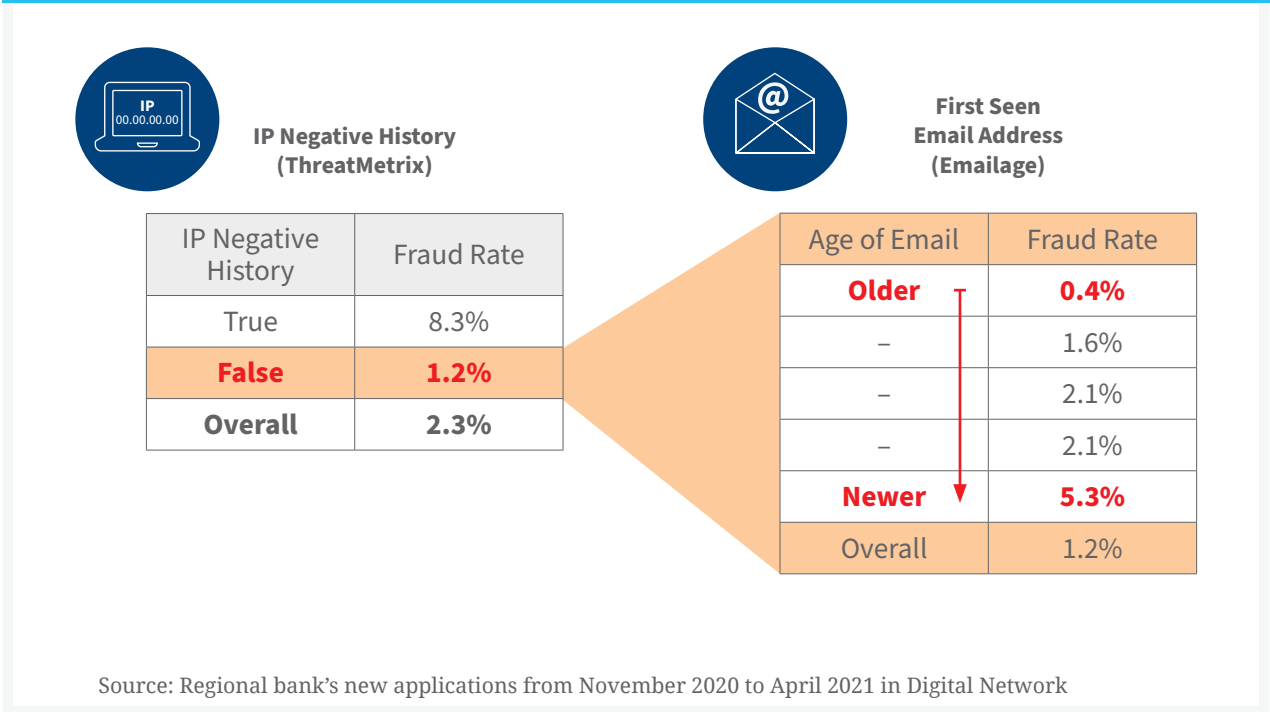
Email and Device Feature Interactions

Further analysis discovered the risk of the *age of the application email* proved **4X** higher when the email was newer versus an email address seen in the last few years. Device characteristics like *CPU Clock Speed* indicate **4X higher** risk for slower (older) devices versus current market devices (faster). *IP Address* is also useful in determining risk when taking into consideration features describing the IP distance from the application address or whether the IP address has been associated with fraud in the past.

Example One

Bivariate or feature interactions expose how each solution domain in the above scenario (Figure 2) diagram can boost the effectiveness of the other. Those IP address appearing to show no historical negative behavior in the ThreatMetrix Digital Identity Network® can be further scrutinized by examining the *Emailage First Seen Email Address*. A significant boost in fraud performance is gained (4X riskier) from implementing this interaction of features. The inverse is also beneficial: for no *IP Negative History* applications, an older email address shows a 0.4% fraud rate.

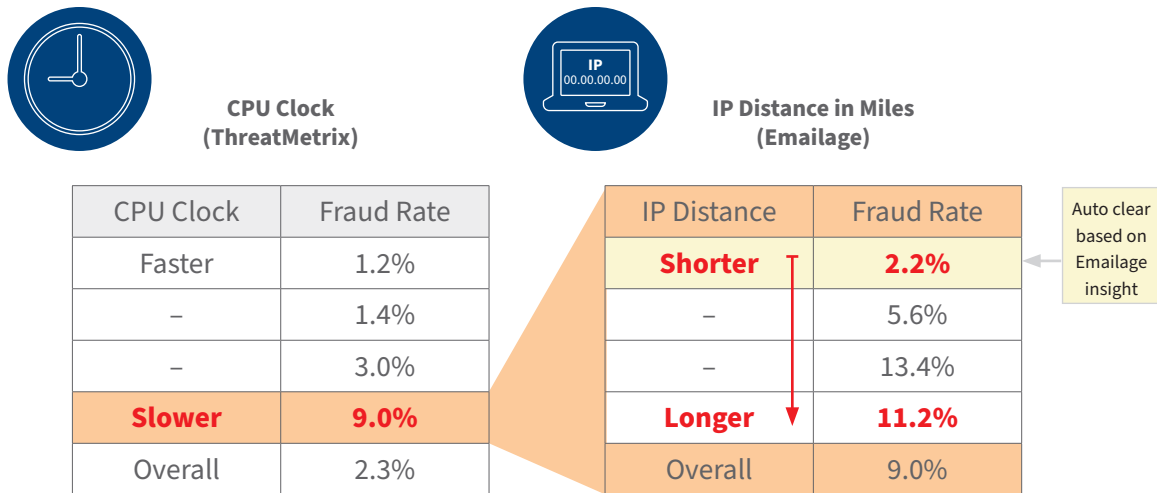
Figure 3: Multi-feature interaction Example #1



Example Two

This second example examines another feature interaction between application device characteristics and IP distance as mentioned above. In this case, the primary indication to fraud risk would be *CPU Clock Speed* from the device. This example highlights how even a non-obvious feature like *CPU Clock Speed* can be used in conjunction with another feature from a different solution domain to increase fraud detection. Evaluating a slow *CPU Clock Speed* and *IP address distance* (from most recently known location), suggests significant performance improvements as well. Higher distances could indicate stolen identity or other software meant to anonymize user web traffic. The farther the distance, the more dramatic the observed fraud loss. Although a slow CPU Clock Speed suggests high fraud losses, shorter *IP distance* indicates a lower risk cohort.

Figure 4: Multi-feature interaction Example #2



Source: Regional bank's new applications from November 2020 to April 2021 in Digital Network

Example Three

From a separate analysis, this third interaction example compares historic LexisNexis Risk Solutions Inquiry Identity Network transaction velocity within Fraud Intelligence where the application landline *Phone number matches Date of Birth* and an Emailage feature quantifying how many days the application email address has been verified. As indicated in Example One, newer application email addresses were significantly more risky than older email addresses and a higher phone number/DOB verification velocity also increased risk. The interaction is especially useful in identifying riskier applications based on the age of the email in a high-risk application velocity band titled: **Newer**. (The inverse perspective is also useful in examining applications using older, more trustworthy email addresses against high phone/DOB application velocity.)

Figure 5: Multi-feature interaction Example #3



**Days Since Email
First Verified
(Digital)**



**Applications with
Phone/DOB Match
(Physical)**

Age of Email	Fraud Rate
Older	1.2%
-	1.4%
-	3.0%
Newer	9.0%
Overall	2.3%

PII Matches	Fraud Rate
Fewer	3%
-	30%
-	53%
More	66%
Overall	5.0%

Source: Regional bank's new applications from November 2020 to April 2021 in Digital Network

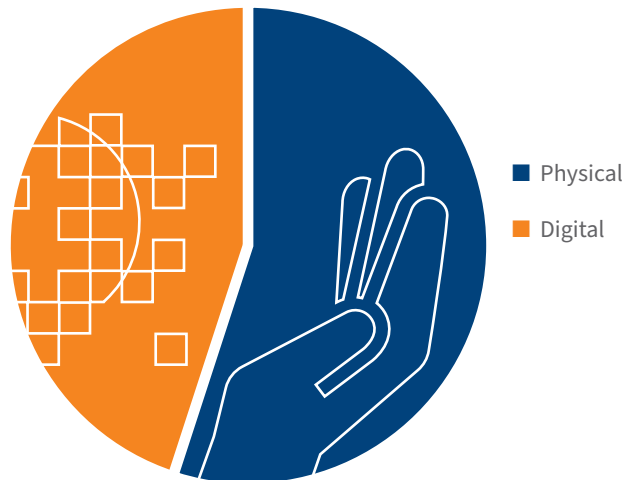
The 360-Degree Integrated Fraud Model

As outlined above, features coming from more than one identity perspective are necessary to form a more holistic view of the identity in question. For new account opening, the information value impact of each feature domain, physical and digital, should be considered. *Variable Contribution by Importance* highlights each data domain's significance in the integrated model and the balance between domains suggests each solution harmonizes with the other. This harmony is further illustrated when comparing the performances of each domain side-by-side.

When examining the Fraud Detection Rate for single sourced custom models on post-booked credit applications representing the top 3% of the riskiest scores (FDR3), each solution performs admirably, but when used together in the same fashion described above, the performance leaps to 77%.

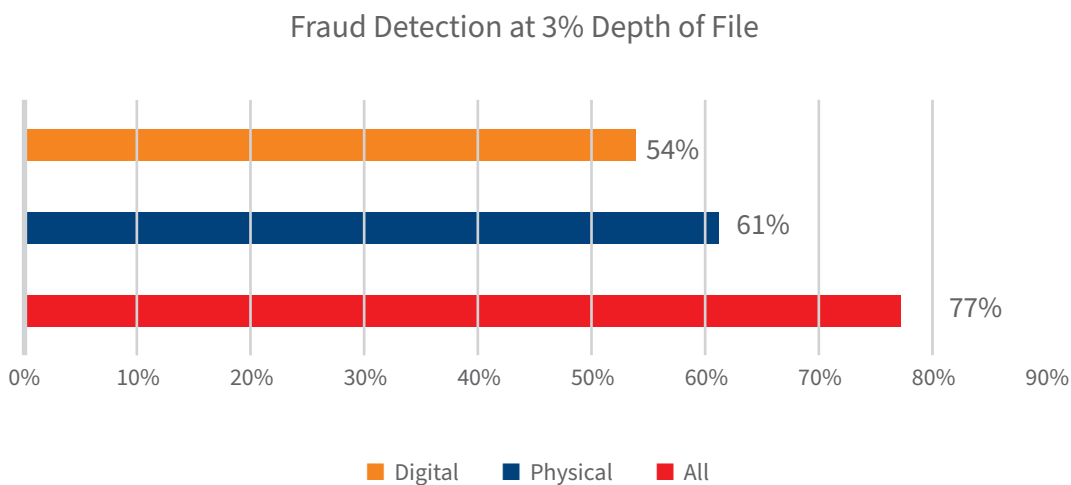
Figure 6: Contributions

Variable Contribution to Account Origination Fraud



Source: Top card issuer's historical new application from 2020 Digital Network

Figure 7: Fraud Detection Comparisons



Source: Top card issuer's historical new application from 2020 Digital Network

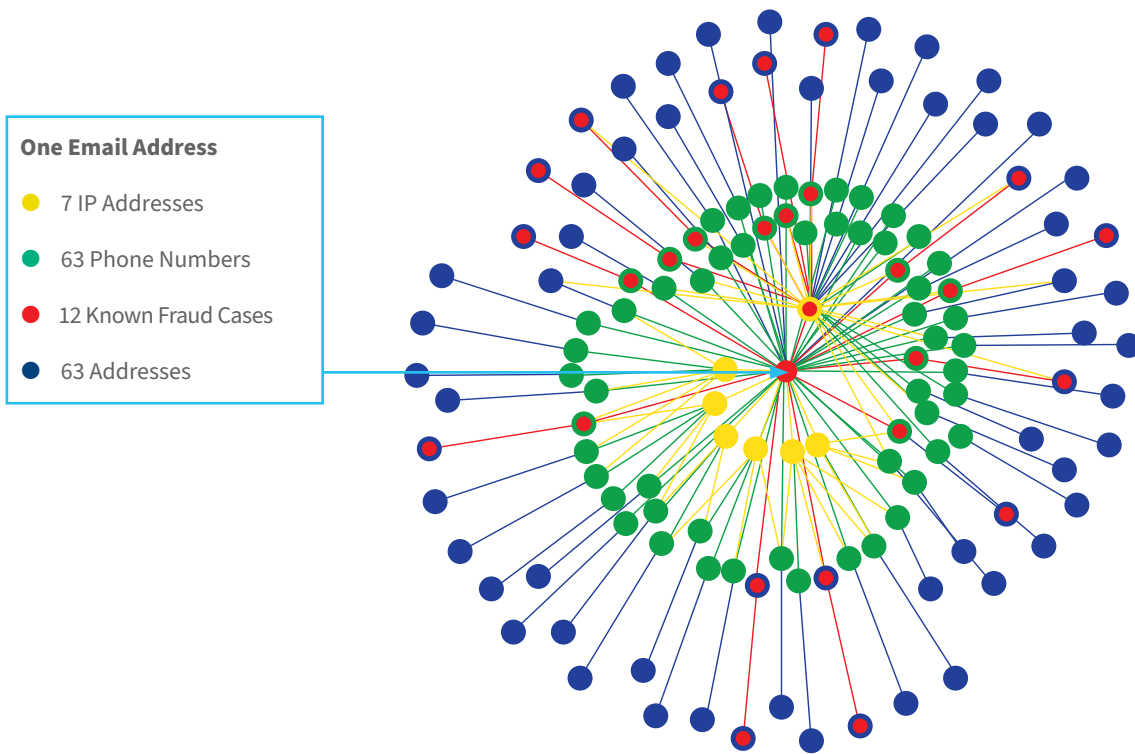
Filling the digital information channel is the Emailage solution driven by an extensive knowledge of email histories while ThreatMetrix leverages digital identities, device data points and behavioral features each at the transactional level. Because each solution is strong at what it solves for, customers do benefit from using one solution, but the real advantage comes with leveraging multiple platforms as each is more sensitive to the differing fraudster tactics. As seen above, combining features from the digital and physical domains produces remarkably better fraud detection than each data domain alone.

Integrated Platform Data

A growing research trend at LexisNexis Risk Solutions takes into consideration identity data from multiple platforms to construct an entity data graph. This data refactoring provides a network-based view instead of focus on a single identity allowing for fraudulent applications to be grouped by common PII elements potentially exposing organized criminal activity. Hallmarks of typical fraud rings include leveraging stolen PII; consolidating contact to a controlled phone, address or email; and uncharacteristic velocity of applications originating from devices frequently with their IP address proxied or obscured with a VPN or TOR.

The graph view has enabled the development of collusion-specific solutions such as the Hot Address and the Fraud Ring Scores within Fraud Intelligence. It has also inspired network insights as well as uncovered fraud ring behaviors and tactics. A fraud ring study for a major bank indicated fraud rings were associated with a 25% fraud rate versus a fraud rate of 5% for those accounts not part of a large collusive effort.

Figure 8: Fraud Network View



Source: Top card issuer's historical new application from October and November 2021

Conclusion

Depending on the specific use case, customers utilizing a multi-layer defense network can expect to greatly improve fraud detection. In our studies, the use of digital identity (ThreatMetrix) and contact (Emailage) scores boost performance up to 21% over a solitary digital solution. When incorporating both digital and physical domains using Fraud Intelligence rates go from 54% and 61%, respectively, to 77% in post-booked fraud detection.

These analyses show that multiple solution domains can increase fraud detection by providing a 360-degree view of the applicant identity allowing the financial institution the opportunity to close the attack vector. The LexisNexis Risk Dynamic Decisioning Platform provides immediate access to most needed solutions and to easily overcome multi-platform integration delays. While criminal tactics will undoubtedly evolve in response to added pressure, LexisNexis Risk Solutions is dedicated to helping our customers win the fight against fraud by continuing the advancement of our analytics and improving our solution effectiveness.

Sources

1. <https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0>
2. <https://www.ftc.gov/news-events/news/press-releases/2021/02/new-data-shows-ftc-received-22-million-fraud-reports-consumers-2020>
3. <https://bankingjournal.aba.com/2021/10/report-synthetic-identity-fraud-results-in-20-billion-in-losses-in-2020/>
4. <https://javelinstrategy.com/2021-identity-fraud-study-shifting-angles>
5. <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Turner-2022-03-17-REVISED.pdf>
6. <https://hbr.org/2021/05/that-dreaded-commute-is-actually-good-for-your-health>

For More Information:
Call 408-200-5755 or email contactusnow@lexisnexisrisk.com to learn more.



About LexisNexis® Risk Solutions

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

All information, data, charts, graphs, figures and diagrams contained herein are for informational purposes only and not intended to and shall not be used as legal advice. LexisNexis Risk Solutions does not guarantee the functionality or features of any LexisNexis Risk Solutions products identified. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.

LexisNexis, LexID and the Knowledge Burst logo are registered trademarks of RELX Inc. Emailage is a registered trademark of Emailage Corp. ThreatMetrix is a registered trademark of ThreatMetrix, Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2023 LexisNexis Risk Solutions Group. All Rights reserved. NXR15857-00-0123-EN