Brought to you by Informa Tech
OMDIA

Publication date:
19 Nov 2021
Author:
Omdia Analyst,
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: FiVerity offers protection against synthetic identity fraud

Summary

Catalyst

FiVerity develops machine learning–based technology to detect synthetic identity fraud (SIF) attempts, which it markets to financial services institutions (FSIs) in the consumer lending sector in the US. Its objective is to secure payments by eliminating both existing and emerging forms of cyber fraud.

Omdia view

As the numbers quoted elsewhere in this report indicate, SIF is a growing problem in the US and worldwide. Even if it restricts its activities to the North American market, FiVerity is in a position to build a significant business, and this will only increase if it goes international.

Why put FiVerity on your radar?

If you are in the consumer lending market in the US, FiVerity should be a candidate for providing fraud prevention data and services. For one thing, it can be deployed as an overlay to supplement your existing systems with its ML-based platform. This is critical, as rule-based systems miss over 85% of likely synthetic identities. Also, the Cyber Fraud Network is a useful tool for sharing much-needed fraud intelligence—alerting banks to SIF within their portfolios as soon as these accounts are detected by any partner in the network.

Market context

The specific area of fraud that FiVerity focuses on is synthetic identity fraud (SIF). This is a growing form of cyber fraud, fueled by the development of the market for stolen credentials on the dark web—which features the 1.3 billion identity elements leaked in the past five years—and the expansion of online commerce that was provoked by the coronavirus pandemic. In the case of the US market in particular, a further factor cited by some observers is the randomization of social security numbers (SSNs), which was instituted by the country's Social Security Administration in 2011.

A synthetic identity is a combination of fabricated credentials where the implied identity is not associated with a real person. Fraudsters create synthetic identities using compromised data such as valid SSNs found on the dark web, combining it with false personally identifiable information (PII). The synthetic may have a real address to which goods may be shipped, and the SSN may appear valid, but the SSN, name, and date of birth combination do not match with any one person.

There are estimates that as much as 20% of credit losses on a typical retail lending portfolio is currently the result of SIF exploits, and one reason this type of attack is so attractive is the fact that it is very difficult to track which identities are in fact fake. Furthermore, the evolution of cloud computing, and more specifically the advent of bots for hire, has made it possible to harness automation in the process of account registration; enabling fraudsters to create tens of thousands of fake identities, build up their credit over time across multiple lenders, then eventually "bust out," taking advantage of one or two of the accounts to defraud institutions of large sums of money. FiVerity has worked with The Federal Reserve to quantify how big the problem of SIF is in the US market, coming up with a figure of $20bn in annual losses from this type of attack, up from $6.7bn in 2016 and $14.7bn in 2018. Beyond this direct financial impact, the crime is often linked to other serious crimes such as money laundering, weapons smuggling, and even human trafficking.

Product/service overview

SIF Detect is a machine learning–based platform that leverages mainly supervised learning to achieve its goals. It can be, and usually is, deployed as an overlay atop existing fraud-prevention systems. The latter tend to be rules-based, which means they are static and so struggle to keep up with the fast-evolving threat landscape in fraud.

The platform is typically also an overlay on, and thus also a complement to, the services of the fraud analyst team. Its purpose, the vendor stresses, is not to substitute the human analyst, but rather to upscale them; keeping the human in the loop and distributing the platform's output across multiple human analysts, for them to collaborate and respond.

FiVerity says the majority of the data collected by SIF Detect is standardized, but it also has APIs for connections to any of its customers' data that is in a proprietary format. It also works with systems integrators to facilitate such connections.

Beyond its fraud detection algorithms, FiVerity's Cyber Fraud Network shares information on synthetic and other forms of fraud detected across its partner banks and law enforcement agencies. This network scales the ad hoc information-sharing that occasionally happens between banks via email and online forums.

To underpin the security of its information-sharing platform, FiVerity adopts a “double-blind” approach, whereby it splits the encryption key across members, so that no single institution holds the complete key to decrypt PII data. This encryption protects its users from violating consumer privacy rules, which has been the primary obstacle to sharing information on suspected fraudsters across FSIs. It also allows financial institutions to maintain confidence in the security of their customer data, as the only companies that can validate a shared profile are the ones that already possess the corresponding PII.

Fraudulent activity identified by SIF Detect is shared by banks in the Cyber Fraud Network without compromising the data privacy of personally identifiable information. This is facilitated through a collaboration agreement with the National Cyber-Forensics and Training Alliance (NCFTA), a public-private partnership that shares cybercrime data between banks and ultimately law enforcement. The two entities have also worked together to raise awareness of SIF, publishing a report entitled *Advisory on Synthetic Identities used by cyber-criminals to infiltrate financial institutions*.

Company information

Background

FiVerity was founded in 2018 by CEO Greg Woolf, who had previously worked as a senior associate at PricewaterhouseCoopers, specializing in risk and assurance for the financial services industry. He also founded several fintech companies focusing on data management for financial asset managers.

FiVerity has so far raised $2m in seed funding, led by Boston-based Mendoza Ventures.

Current position

FiVerity focuses specifically on the consumer lending market (i.e., issuers of credit cards, automotive and personal loans), because this is the area where synthetic identity fraud is most prevalent. It currently operates only in North America, though clearly fraud prevention technology is relevant globally. The target audience for SIF Detect is consumer lending institutions with over $8bn in assets, and banks of all sizes can join the Cyber Fraud Network.

SIF Detect went on general availability in 2021. It is a machine learning–based platform for fraud and cyber analysts to use during the credit application process. In August this year, FiVerity unveiled the Cyber Fraud Network, which is a community designed to improve the collective cyber fraud knowledge of financial institutions, regulators, and law enforcement by facilitating the secure exchange of intelligence on suspected fraudsters, without disclosing PII.

FiVerity says the idea for the Cyber Fraud Network came out of work it was doing with a think-tank comprising a number of risk and compliance officers from FSIs in its native Boston. The information-sharing network uses AI and machine learning to detect sophisticated forms of cyber fraud and deliver proactive threat intelligence to banks and law enforcement agencies. Importantly, the network’s "double-blind" encryption of PII protects its users from potentially exposing private consumer information, which is a risk inherent in sharing information informally.

It is accessed via API integration and enables each individual FSI to strengthen its defenses by alerting them to fraudulent activity detected throughout the network. This multiplies each user's ability to identify and learn from new fraud patterns.

The two products complement one another, with FiVerity offering SIF Detect on top of the Cyber Fraud Network. In addition to annual subscriptions, FiVerity offers a lightweight analysis to identify SIF accounts within existing loan portfolios.

Future plans

While it is currently focused entirely on the US market, FiVerity intends to expand internationally, with both Europe and Asia in its plans. FiVerity is working to identify other forms of cyber fraud experienced by banks and credit card companies.

Key facts

Table 1: Data sheet: FiVerity

Product/Service name	SIF Detect Cyber Fraud Network	**Product classification**	Cyber fraud defense
Version number	2.3 1.1	**Release date**	March 2021 August 2021
Industries covered	Financial services, specifically consumer lending	**Geographies covered**	US & Canada
Relevant company sizes	Enterprise	**Licensing options**	Portfolio analysis on project basis Annual subscription
URL	www.fiverity.com	**Routes to market**	Direct System integration partners Loan origination system partners
Company headquarters	Boston, Massachusetts, US	**Number of employees**	20+

Source: Omdia

Analyst comment

While synthetic identity fraud is clearly enjoying rapid growth, the fraud prevention market is also awash with vendors large and small, all of them vying for the attention of FSIs. Thus, one of the challenges faced by FiVerity is how to gain visibility in such a crowded market. In this context, Omdia applauds its strategy of working with the Fed, as well as with organizations such as the NCFTA, both to increase awareness of SIF and to raise its own profile. FiVerity's development of a solution that protects PII is also a critical catalyst to getting adoption from FSIs.

Information-sharing mechanisms in the financial sector are not new, of course. Indeed, the FSIs themselves have done a lot of work in this area, particularly in the context of the Financial Services Information Sharing and Analysis Center (FS-ISAC), and Omdia wonders whether, down the road, the Cyber Fraud Network might not be merged with, or subsumed into, some broader initiative by FS-ISAC, with the latter taking over its data curation. This might be a useful trade-off for FiVerity, if it can offer SIF Detect to the entire membership of FS-ISAC in exchange.

Omdia also applauds the vendor's decision to focus only on the US market, at least for the time being. First, because there is more than enough market potential there, particularly for a company with limited head count and only modest funding. There may also be other unique challenges in different geographies, such as the question of data residency within the European Union, so it is a wise move to walk before it tries to run.

At the moment, Omdia sees no clear winner in the market for SIF prevention technology, and of course, FiVerity's ability to work alongside and supplement a customer's existing fraud prevention tools is a distinct advantage.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Bryan Richardson and Derek Waldron, "Fighting back against synthetic identity fraud," McKinsey & Company, www.mckinsey.com/business-functions/risk-and-resilience/our-insights/fighting-back-against-synthetic-identity-fraud, 2 January, 2019.

FedPaymentsImprovement.org, "Payments Fraud Insights: Synthetic Identity Fraud in the U.S. Payment System," https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf (July 2019)

FedPaymentsImprovement.org, "Payments Fraud Insights: Detecting Synthetic Identity Fraud in the U.S. Payment System," https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-october-2019.pdf (October 2019)

FedPaymentsImprovement.org, "Payments Fraud Insights: Mitigating Synthetic Identity Fraud in the U.S. Payment System," https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020.pdf (July 2020)

FiVerity, "NCFTA & FiVerity Security Bulletin: Advisory on Synthetic Identities used by cyber-criminals to infiltrate financial institutions," www.fiverity.com/bulletin1.pdf (November 2020)

FiVerity, "FiVerity 2021 Synthetic Identity Fraud Report," www.fiverity.com/resources/sif-report-2021 (October 2021)

ID Analytics, “Slipping Through the Cracks: How Synthetic Identities are Beating Your Defenses” (November 2019)

ITRC 2020 in Review: Data Breach Report (January 2021)

Author

Rik Turner, Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com