FRAUD FIGHTERS MANUAL

FOR FINTECH, CRYPTO, AND NEOBANKS

Presented by Unit21

"The most important thing is to be aware of the types of fraud that exist and to be very vigilant about putting human effort into analysis and critical thought."

— Robert Reynolds, Pinwheel

Foreword

Fraud is a taboo topic in the Fintech world.

Unfortunately, many prefer to hide the subject behind closed doors rather than discuss it publicly.

However, as someone who has been fighting against fraud since 2009, I know the importance of addressing the issue out in the open. When I started my journey, the Financial Crime Unit I was part of was primarily focused on unauthorized card purchases, classic “card not present” fraud, and counterfeit card fraud.

Over the years, I have held various positions in the industry, from fraud operations to fraud analytics, and have seen first-hand the impact of fraud on businesses. In late 2019, I took on the responsibility of leading the fraud prevention program in a newly established Neobank, and I asked myself the question: “Where do I start?”

Because the Financial industry is rapidly evolving with the emergence of new technologies, this has led to a rise in fraudulent activities and various ways in which fraud can be carried out. As a result, it has become increasingly difficult to clearly define all the aspects of fraud and determine the associated losses. What one Fintech company may consider a typical cost of doing business may have a more significant impact on another company’s profitability.

What Fintechs consider when defining a fraud loss very much depends on the ecosystem they’re operating in. In an industry where growth and scale play a significant role in early success, creating internal alignment between product, marketing, customer success, and senior management around fraud prevention is no easy task.

That’s why I am excited to introduce this book, which Unit21 collaborated on with some of the brightest minds in the industry to shed light on the dark world of Fintech fraud, and provide practical solutions to mitigate risks and create interdepartmental continuity.

Through a series of informative and engaging chapters, the authors give readers a behind-the-scenes glimpse into the industry as a

whole, and into the thought processes of various frontline professionals who deal with fraud on a daily basis.

The authors' expertise and knowledge of fraud detection and prevention are evident throughout the manual. They provide insight regarding the challenges that Fintechs face, and ways to overcome them. By connecting the dots between the problems discussed in the book with the difficulties Fintechs are experiencing, the authors provide a blueprint for readers to follow that is both fascinating and educational.

As a leader in the fraud detection and prevention space, Unit21 felt obligated to make this book a valuable resource for Fintech founders and risk professionals looking to understand how instances of fraud are perceived, managed, and avoided at other organizations, as this information is not readily available.

We combined engaging storytelling with fact-based research to make for an illuminating and thought-provoking read that is essential for anyone hoping to expand their depth of knowledge, explain the complexities of fraud prevention, or enhance their fraud prevention strategies. We believe that by surfacing these stories, the challenge of Fintech fraud will be reduced.

I hope this book will help Fintechs approach the subject with confidence, knowing that it will not hurt their scale but rather contribute to healthier growth. It's time to break the taboo and begin tackling fraud head-on. This book is an excellent place to start.

Alex Faivusovich
Head of Fraud Risk, Unit21

About Unit21

The task of managing fraud risk is growing in complexity. From dealing with an ever-growing volume of alerts and relying on engineering teams to update static systems, fraud fighters are disadvantaged in a world where bad actors are more well-funded, technologically savvy, and agile than ever before. Unit21 helps teams tackle these problems head-on with a flexible no-code infrastructure for detecting and preventing fraud.

Backed by Google, Tiger Global Management, and other leading investors, Unit21 redefines how risk teams fight financial crime. Unit21's fully customizable platform provides a simple API and dashboard for detecting, investigating, and reporting fraud, money laundering, and other sophisticated risks across multiple industries.

Combining onboarding orchestration, transaction monitoring, and suspicious activity report (SAR) case management, Unit21 streamlines every aspect of risk operations.

For more information, visit www.unit21.ai.

Special Thanks

We wanted to offer a special thanks to all of Unit21's customers who have been on the front lines, working day in and day out to keep their organizations and the greater world safe from financial crime. You have inspired us to write this book, and we can't acknowledge you enough for the critical work you do every day as fraud fighters.

In addition, we'd like to formally thank all of our contributors for sharing their unique experiences, the Unit21 marketing team for their efforts in brainstorming, imagining and bringing this project to light, and Unit21's CEO, Trisha Kothari, for continuously dreaming big and encouraging us all to achieve things we've never thought possible.

#TeamworkMakesTheDreamWork

Publishers

Shana Haynie, Head of Content, *Unit21*
Alex Faivusovich, Head of Fraud Risk, *Unit21*
Trisha Kothari, Co-Founder & CEO, *Unit21*
Clarence Chio, Co-Founder & CTO, *Unit21*
Aditya Vempaty, Head of Marketing, *Unit21*

Contributors

Robert Reynolds, Head of Product, *Pinwheel API*
Kevin Yang, Core Engineer, *Nibiru Chain*
Kenny Grimes, Head of Risk Strategy & Analytics, *Mercury*
Tanya Corder, Compliance Manager, *Treasury Prime*
Zach Pierce, Risk Ops Lead, *Lithic*
Rajeev Muppala, Head of Risk Operations, *Brex*
Ali Rathod-Papier, Head of Financial Crime Compliance, *Brex*

Creative Direction

Garrett Kline, Head of Brand & Design, *Unit21*

Book Designer

Darren Chan, *Darren Chan Design*

Close your eyes, take a deep breath, and think about the word "fraud." What comes to mind?

There's no denying it—the term fraud holds a severely negative connotation in today's modern world. Even though it is a common (and some might argue, expected) occurrence in the business landscape, talking about it is still highly taboo for organizations in the financial services industry.

In fact, we could suffice it to say that many organizations view fraud as the "f-word,"a bad turn of phrase that should never be publicly uttered for fear of reputational ruin. All references to fraud or acknowledgments of its existence should be limited to conversations behind closed doors, lest society catch wind of the dirty truth that fraud happens and many types[1] are happening at an increasing rate year over year.

However, fraudsters continue to become more sophisticated, and companies—especially those operating in the Fintech and financial industries—need to gain a deeper understanding of the associated risks and what steps they can take to prevent fraud. And that means overcoming this fear of public shame and discussing the problem openly.

It may sound cliche, but crime tends to hide in the shadows. The best way to catch them is to shine a light in their direction, and this can't be done without knowing where to look.

To support this objective of surfacing shuddered strategies, tactics, processes, and best practices, we spoke directly to many experts at leading Fintech companies and compiled their views into this manual. Their unique perspectives, broad set of disciplines, and enthralling stories help us add color to topics like synthetic identities, risk management, cryptocurrency, account takeover, and more. In each chapter, you'll find an overview of the topic infused with quotes from our contributors, along with a complete Q&A section that showcases the ebb and flow of each conversation.

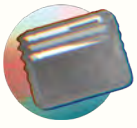
While each chapter is self-contained, we recommend reading them in order, as each chapter builds on the one that came before it to create a broad picture of the current state of fraud, along with practical ideas for how to combat it effectively.

Before we get too far ahead, it's critical to understand where we are with regard to fraud and some of the trends that Fintechs are experiencing as they work to balance safety with scale.

Fraud in the 2020s

The recent rapid technological advancements that have transformed the way we live our lives have also given fraudsters a new playing field. With the rise of online banking, electronic payments, and cryptocurrencies, fraudsters now have access to a broader range of assets and channels to conduct their illegal activities than they did a decade ago. It is crucial that individuals and organizations alike stay vigilant and adopt rigorous security measures to protect themselves from these threats. The following takes a look at four key areas influencing the current state of fraud.




	Credit Card	*Account Takeover*	*True Identity*	*ACH/Debit*	*Fake Identity*
Percent of digital fraud (2022)	***6.5%***	***6.3%***	***6.2%***	***6.0%***	***5.3%***
Volume Change (2019-22)	***76%***	***81%***	***81%***	***122%***	***132%***

1. The Growth of Friendly Fraud

Unlike other types of fraud—we'll cover those in Chapter 1—friendly fraud is committed by someone close to the customer (like a family member). A typical example is a child using their parent's payment information to make purchases. Because the fraudster has access to legitimate payment information, friendly fraud is difficult to detect and prevent. It's also surprisingly common. According to a survey for the 2023 Digital Trust & Safety Index put together by Sift, "16% of consumers admit to having committed payment fraud/knowing someone who has.[2]"

This type of fraud can result in significant financial losses for businesses that rely on online transactions. This threat requires proactive measures from companies to protect themselves against potential losses.

2. More Digital Channels

The growth in digital channels has made it easier for fraudsters to apply for credit and other financial products online using stolen identities. According to the TransUnion 2023 State of Omnichannel Fraud Report: an "80% increase in digital transactions resulted in 80% growth in suspected digital fraud attempts globally from 2019 to 2022.[3] "Synthetic identities, which we'll discuss in the second chapter, are difficult to detect because they are often based on real information, and are also more common because of this increase in digital channels.

3. New Technology

Technological advances have given fraudsters new opportunities too. Breakthroughs in artificial intelligence and machine learning simplify the process of bypassing security measures, while increased use of cryptocurrencies and blockchain technology, which we'll cover in Chapter 3, makes it harder to catch and trace illegal activities. The industry around these technologies is growing rapidly—for example, AI is expected to be a trillion-dollar industry by 2030[4]. More and more products connect to the Internet of Things (IoT), and the increasing amount of data generated by connected devices has made it more difficult for companies to identify and prevent fraudulent activity.

The growth of the dark web created a new industry of fraud and enabled bad actors to commit fraud on a larger scale. The dark web hosts illegal marketplaces, allowing fraudsters a place to buy and sell sensitive information like stolen identities and credit card numbers.

4. The Pandemic

The COVID-19 pandemic has had a significant impact on the world, and one of its many repercussions has been the increase in fraud. As people were spending more time and money online due to lockdowns and social distancing measures, more opportunities for fraudsters to take advantage of unsuspecting victims arose. When the pandemic hit, and the government began rolling out pandemic relief programs, there was more money available for fraudsters to exploit. This contributed to increased fraudulent activities, ranging from phishing scams to identity theft.

In 2022, prosecutors working on fraud cases involving pandemic relief funds said that pandemic fraud was so rampant that in two years, they'd only gotten started[5] on their stack of cases. According to the FBI's annual Internet Crime Report, complaints of internet fraud rose from 467,361 in 2019 to 791,790 in 2020[6]. In 2021 and 2022, that that number has increased to over 800,000.

Knowledge Is the Key to Prevention: What You'll Learn in This Book

It's clear that fraud isn't going down anytime soon.

Organizations of all types have a pressing need to identify potential fraudsters to protect themselves against the negative consequences of financial disruption, but this is especially important in Fintech, given the current climate.

In order to do this, risk management teams must employ a variety of techniques and strategies. One such strategy is to use advanced data analytics and software to detect patterns of behavior that may indicate fraudulent activity. Another approach is establishing internal controls that make it more difficult for fraudsters to carry out their schemes. Additionally, organizations can invest in training and development programs for their employees to help them recognize potential red flags and report suspected fraud in a timely manner. By taking these steps, organizations can minimize their risk of financial loss and retain the trust of their stakeholders.

We've divided the book into six chapters designed to give you insight into how other organizations are actively handling each of the following concepts. We recommend you read every chapter for a detailed rundown on each topic:

Chapter 1: Know Your Fraudster

We begin the book by introducing the three types of fraud and the seven archetypes of fraudsters so you can spot a fraudster a mile away. By knowing the different types of fraud and recognizing the various archetypes of fraudsters, individuals and organizations can identify patterns of behavior that suggest fraudulent activity and take appropriate action to prevent further damage.

Robert Reynolds of Pinwheel offers examples of surprising fraud instances and discusses the most vulnerable processes fraudsters most frequently target.

Chapter 2: Compromised and Synthetic Identities

In Chapter 2 we dive into stolen identities, synthetic identities, and how fraudsters gain access to sensitive information through dark web marketplaces, social engineering methods, and deep fakes. We recommend a three-pronged strategy for financial institutions to combat fraud, including custom onboarding workflows, continuous monitoring, and case management solutions.

We'll also discuss how Know Your Customer (KYC) and Know Your Business (KYB) strategies are used by organizations to collect and process personally identifiable information about their customers or business partners. This information is then used to verify their identities, which can help prevent fraud before it occurs. KYC/KYB strategies also use behavioral analysis to identify potential fraudsters by looking for patterns of behavior that suggest fraudulent activity.

Unit21's own Alex Faivusovich looks at why it is important to understand the various methods that fraudsters use to gain access to consumer information. One of the most common strategies is phishing, which involves sending out fake emails or messages in an attempt to trick someone into providing sensitive information.

Other methods of social engineering rely on psychological manipulation and malware, which is malicious software that can be installed on someone's computer without their knowledge.

Chapter 3: Cryptocurrency Fraud

Cryptocurrency fraud is a unique challenge. The decentralized nature of cryptocurrencies and the lack of regulation in many jurisdictions make it difficult to detect and prevent fraudulent activity. In addition, the anonymity of cryptocurrency transactions makes it easy for fraudsters to use stolen identities or create synthetic identities to conduct illegal activities.

Kevin Yang of Nibiru Chain discusses the importance of physical security measures, such as physical wallets and USB keys, as well as the need for organizations to thoroughly vet cryptocurrency partners and protect themselves with robust KYC/KYB policies. Kevin also explores the increasing regulations around cryptcurrency and how they may make the market more stable.

Chapter 4: Account Takeover (ATO) Fraud

Account takeover (ATO) is a type of fraud that occurs when an attacker gains access to a user's account by stealing their login credentials. Once inside, the attacker can make unauthorized transactions, steal sensitive information, or even take over the account completely.

Kenny Grimes of Mercury and Tanya Corder of Treasury Prime dive into the four stages of ATO and the red flags to watch out for. They also share strategies to prevent ATO, such as double-checking vendor purchases, staying on the lookout for unusual account activity, using a password manager, changing passwords regularly, and enabling 2FA wherever possible.

Chapter 5: Fraud Detection 101

Organizations must implement various tools to help their risk management teams catch and prevent fraud. These tools include sound user onboarding systems that help verify the identities of new customers or business partners, transaction monitoring tools that flag suspicious activity in real time, and case management systems that help risk management teams investigate potential fraud and take appropriate action.

When it comes to preventing fraud and detecting suspicious activity, there are a variety of solutions that can be effective. One such tool is the rules engine, which allows Fintechs the ability to use logic to identify and act on potential threats. In addition to staying on top of emerging issues, these technologies also help organizations meet regulatory requirements and maintain compliance with industry standards.

Zach Pierce of Lithic shares his thoughts on why it is critical to regularly review and update internal policies and procedures to stay ahead of emerging threats, how to ensure that best practices are being followed, and which tools are best for Fintechs at certain stages.

Chapter 6: Risk Operations

One important aspect of risk management involves collaborating with other departments to ensure that risk is being properly identified and addressed across the organization. By working together, teams can share information and insights that may not be apparent from a single perspective.

Rajeev Muppala and Ali Rathod-Papier of Brex speak about how an organization's structure or industry can affect its risk operations needs. They also share their thoughts on how the risk operations team should be staffed with individuals who have the skills and knowledge necessary to identify and respond to emerging threats. In addition to building a strong team, they also express that it is imperative for organizations to collaborate with other departments to build better risk management across the organization.

Face Fraud Head On, Eyes Open

As noted earlier, fraud is a subject that people feel the instinct to avoid. It brings up feelings of fear that we'd rather ignore. But by staying informed about emerging threats and adopting best practices for fraud prevention, organizations can better protect themselves against financial disruption and maintain the trust of their stakeholders.

The following six chapters should act as a jumping-off point for fraud fighters everywhere to identify gaps in their current programs and inspire innovation where needed to fight financial crime effectively. The first step in this process is to gain an understanding of the characteristics of fraudsters who perpetrate various types of fraud.

1. Akin, Jim. "Identity Theft Is on the Rise, Both in Incidents and Losses" Experian, Experian, 17 Nov. 2022, https://www.experian.com/blogs/ask-experian/identity-theft-statistics.

2. "Q1 2023 Digital Trust & Safety Index." Sift Resources, 22 Mar. 2023, https://resources.sift.com/ebook/q1-2023-digital-trust-safety-index-payment-fraud/.

3. "TransUnion 2023 State of Omnichannel Fraud Report." TransUnion, https://www.transunion.com/content/dam/workfront-assets/truportfolio/GFS-22-F125939-TruVa-2023OmnichannelFraud-RPR-US_EN-US.pdf.

4. Thormundsson, Bergur. "Market size and revenue comparison for artificial intelligence worldwide from 2018 to 2030 " Statista, 27 June 2022, https://www.statista.com/statistics/941835/artificial-intelligence-market-size-revenue-comparisons/.

5. Fahrenthold, David A. "Prosecutors Struggle to Catch up to a Tidal Wave of Pandemic Fraud." The New York Times, The New York Times, 16 Aug. 2022, https://www.nytimes.com/2022/08/16/business/economy/covid-pandemic-fraud.html.

6. Federal Bureau of Investigation Internet Crime Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.


KNOW
YOUR
NEIGHBOR

“The most important thing is to be aware of the types of fraud that exist and to be very vigilant about putting human effort into analysis and critical thought.”

— Robert Reynolds, Pinwheel

Fraud and fraudsters come in many flavors: First party and third party. External and internal. Some are driven by opportunity, while others carefully plan their attack. But every type of fraudster relies upon a veil of deception. Once that deception is pierced, the threat is mitigated.

Know Your Customer (KYC) and Know Your Business (KYB) regulations provide guidelines through which organizations can better identify potential fraudsters and protect themselves against the financial disruption of fraud.

Fraud is Everywhere—and Difficult to Defend Against

Fraud is on the rise. According to PwC's Global Economic Crime and Fraud Survey [7]2022, 51% of responding organizations reported experiencing fraud within the last two years, the highest level in 20 years. In its 2022 Fraud and Industry Trends[8], LexisNexis attributes rising fraud to a variety of societal accelerants, including digital transformation, increased automation, and disruptive new technologies.

But organizations are not helpless. Behind every fraud, there's a person. By understanding—and identifying—fraudsters, an organization can develop its first and most critical line of defense.

We interviewed ***Robert Reynolds*** to find out more about fraudsters, how they operate, and how they can be detected through advanced KYC/KYB processes. Robert Reynolds is Head of Product at Pinwheel (pinwheelapi.com), a B2B company that helps facilitate connectivity between institutions and payroll systems. Pinwheel's mission is to enable greater financial outcomes for end consumers by creating greater access to credit—and simplifying data-sharing patterns between consumers and financial institutions.

Robert has spent 15 years focused on lending, Fintech, consumer lending, and banking-as-a-service. His fraud-related-knowledge extends to unsecured business loans, auto loans, and credit loans across the US, UK, Australia, and Canada.

The Many Types of Modern Fraud

How do you defend yourself against an attack when you don't know where it will come from—or who it will be? There are many types of fraud, perpetrated by many types of fraudsters. The modern organization faces global exposure and rising advancements in tech.

First-party vs. Third-party Fraud

According to Robert, one of the most important things a company can do to identify bad actors "is to be aware of the types of fraud that exist." Based on that knowledge, organizations can then develop dynamic policies to stop fraud in its tracks. Fraud is frequently categorized as first party or third party, depending on how the fraudster presents their identity. In 2021, the Federal Trade Commission[11] received close to 1.4 million reports of identity theft from customers.

First-party fraud

A fraudster knowingly misrepresents themselves or their actions for material gain. A car salesman sells a car that they know will break down in a few days—and tells the customer that there's nothing wrong with it. An executive writes a large check they know will bounce to secure a contract. Robert points out that "in a lending environment, it's sometimes called friendly fraud as well."

Third-party fraud

A fraudster uses someone else's personal information for material gain. "It can manifest either primarily digitally—in the form of information gleaned from the dark web or stolen information from phishing websites—but it can also manifest physically in the real world," says Robert. An identity thief uses someone else's information to procure a car loan, which is then never paid. Or they pretend to be an executive and write a large check to themselves.

With the right identity verification processes in place, organizations can detect fraudsters in all shapes and forms to prevent attacks from taking a serious toll.

The 7 Fraudster Archetypes

Fraudsters differ in origins and levels of premeditation. A fraudster could be a teenager idly trying out Social Security numbers they purchased online—or a well-planned group of malicious attackers for whom committing fraud is their day job. There are likely hundreds of thousands of fraudsters out there. But they tend to fit into one of seven major categories.

1. The Thief

The Thief is an impulsive individual generally conducting a reckless, one-off fraud. A young partier discovers a credit card on the dance floor and uses it to buy just a few drinks. An employee sees a coworker's phone unlocked—and takes the opportunity to CashApp themself hundreds of dollars.

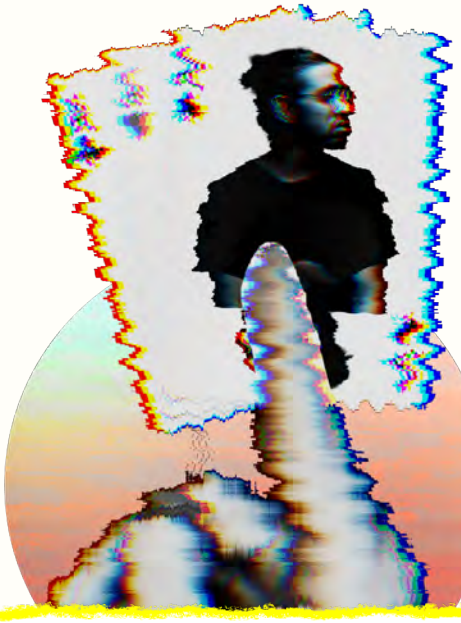
Thieves act when the opportunity arises. But any time an opportunity does arise, the Thief might be there. They can be thwarted by most rudimentary identification checks.

Environment: External
Premeditation: None
Fraud Type: First-party

2. The Con Artist

The Con Artist lies to get their way—whether they have privileged information or not. A person walks into a bank and insists that the ATM short-changed them, getting the teller to hand over money that they weren't actually owed. A vendor says they haven't been paid, even though they were.

Con Artists exploit human nature by lying about their identity and situation. They are defeated through checks and balances. The proper systems and processes make it harder to manipulate an individual.



Environment: Internal or External
Premeditation: Moderate
Fraud Type: First-party

Environment: External
Premeditation: Moderate
Fraud Type: First-party

3. The Disguise Artist

The Disguise Artist is using another person's identity to give themselves access to resources. A cybercriminal sends out an email as a C-suite executive to have an executive assistant wire them money. A vendor forges paperwork stating that a former partner agreed to a contract that was never actually negotiated.

Disguise Artists don't usually have any familiarity with the individual whose identity they are stealing. Rather than having privileged information (such as a Social Security number), they use social engineering and confidence tricks. Identity verification and processes will quickly reveal their deception.

Environment: Internal or External
Premeditation: Moderate
Fraud Type: First-party

4. The Impersonator

The Impersonator misrepresents who they are for profit—and they usually have a plan. A parent with a bad credit score uses their child's identification to open a credit account. A business owner forges their partner's signature on documents to take out loans.

An Impersonator goes a step further than the Disguise Artist by using actual personally identifiable information to pretend to be someone. Thus, it's not enough to simply verify that an "identity" is real; to protect against an Impersonator, you must also verify that the person is who they say they are. This is particularly difficult in the case of family fraud, as relatives are frequently able to take on an identity quite easily.

When Fraud Comes From Inside The Household

"Family fraud is when you have someone who is very close to the victim and can easily represent their identity, misrepresenting the state of their interest or needs," says Robert. "And that could be a spouse, caregiver, or another family member."

5. The Opportunist

The Opportunist exploits ad hoc processes or system vulnerabilities. A retail investor realizes that a stock-trading app is giving them free stocks every day, instead of once, and continuously exploits the error. A vendor sends fewer inventory items in a shipment after noticing they haven't been counted.

An Opportunist does not misrepresent who they are—and they don't set out to commit fraud or even thievery. Rather, they take advantage of exploits that already exist to get away with small things that they should not. To identify Opportunists, not only does identity need to be tracked, but also behavior.

Environment: Internal
Premeditation: None
Fraud Type: First-party

Environment: External
Premeditation: High
Fraud Type: Varies

6. Organized Criminals

The Organized Criminal is working with a professional team. An organized cyber-criminal gang conducts a DDoS attack on a cryptocurrency exchange with the goal of gaining access to the system. A ring of multiple identity thieves represents itself as a business to a bank, walking away with a sizable loan.

Organized Criminals have resources. They are extremely dangerous but comparatively rare. They have the tools and processes to conduct significant damage—but they can be defeated by the same identity-driven protocols as other types of fraudsters.

Environment: External
Premeditation: High
Fraud Type: Varies

7. The Shady Business

The Shady Business is a business knowingly operating outside of regulatory compliance or even the law. A company pushes forward with a project that will incur major environmental compliance issues. A business deals with individuals that it knows are committing fraud or forgery.

Shady Businesses bring risk to banks and other financial institutions. Organizations have to vet and monitor their business relationships in addition to their customer relationships to avoid financial and legal consequences.

Know Your Customer (KYC) and Know Your Business (KYB) Strategies

Once you know your fraudsters, it's time to detect them—through identity verification and due diligence. KYC/KYB regulations form the framework of the necessary standards and processes.

Know Your Customer

KYC is a regulatory requirement for financial institutions. FinTech companies, banks, and credit unions must identify individuals before taking them on as customers. KYC strategies protect against the Disguise Artist, Identity Thief, and Organized Criminals.

Compared to KYB, KYC is fairly easy to implement. Under KYC, you must:

- ***Collect (and protect) personally identifiable information (PII).***
- ***Process the information internally.***
- ***Confirm that the information is valid and accurate.***

Robert highlights the importance of constantly revising KYC strategies, particularly when dealing with third-party fraud. "You're effectively fighting against an enemy with unlimited time and unlimited resources," he says. "The idea that they're not going to change their strategies in response to your tactics is somewhat foolhardy. You need dedication to updating and changing."

For most customers, identity verification processes are easy to manage and well-tolerated. For financial institutions, solutions are available to manage and streamline the verification process end to end.

Know Your Business

KYB refers to the process of verifying any vendors or business entities that the organization does business with. KYB strategies are harder to implement because they require a higher level of due diligence. As Robert points out, "in the case of KYB, where you're verifying the legitimacy of a company to assess the risk of doing business with them, that's more acutely associated with the actual legitimacy of the business. In that sense, just meeting the bare minimum of the legal requirement is not going to be nearly enough to actually prevent and mitigate fraud."

Under KYB, organizations must collect and process large volumes of data. They must investigate and confirm the company's financial, legal, and regulatory compliance information—and they must complete background checks on major stakeholders. In short, "KYB success relies very, very heavily on governance and process control to ensure compliance," Robert says.

KYB strategies protect financial institutions from large-scale fraud, such as those conducted by the Organized Criminal or the Shady Business. Critically, KYB prevents a financial institution from doing business with a company that could be otherwise involved in breaking the law.

Frictionless Fraudster Management

All fraudsters have something in common: they are lying. A fraudster misrepresents who they are, what they want, or what they can provide. Confirm all the facts to understand the end game of the fraudster—and to prevent them from getting what they want.

Today, it's not enough to simply meet the standards of KYC/KYB regulations. Companies must engage in advanced techniques such as behavioral analysis to identify the most clever of frauds.

Advanced KYC/KYB Strategies

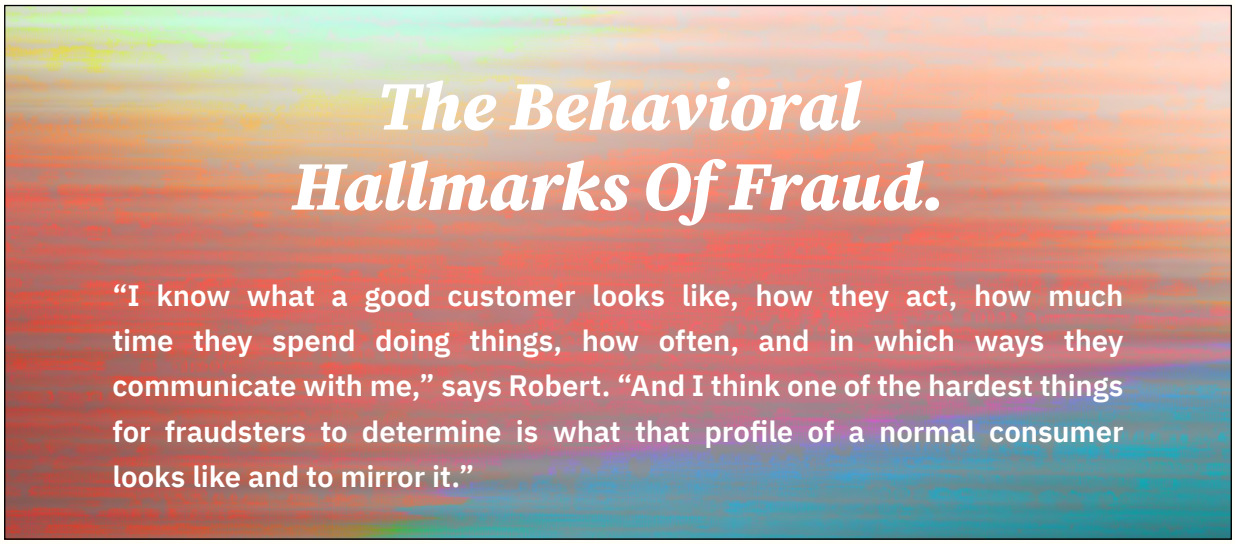
Robert points out that "if you want no fraud, you'll have no volume run through your business." Reducing fraud frequently means adding friction—and adding friction reduces volume. But there are complex KYC/KYB practices that operate behind the scenes, effectively identifying the hallmarks of fraud before the fraud is realized and friction created.

For KYC, companies can use contextual and behavioral clues to identify potential fraud. Is a new device being used? Is the user in a new location? Is the email address new—is the phone number verified? These are clues passively collected without interruption to the customer.

"This requires true human intervention, like evaluating and categorizing fraud into different categories and coming to good definitions," Robert explains. "And being diligent about sampling enough of your consumer data to not just trust the definitions

you have in place but staying vigilant and trying to observe new types of fraud."

For KYB, companies have to be more discerning. They need to use third-party solutions to ensure that the business isn't just active—but that it's trustworthy. And like advanced KYC policies, the best KYB strategies use behavioral modeling and real-time detection. Are unusual behavioral patterns occurring under the account? Is the account asking for something it has never asked for before?



Key Takeaways:

- ***There are many types of fraudsters, with varying degrees of organization and competency***
- ***On both a customer and business level, your goal is to catch bad actors while letting good actors through—as seamlessly as possible***
- ***Using advanced KYC and KYB strategies like behavioral modeling and real-time detection paired with continuous human intervention are critical steps for success***

It is one thing to be aware of the various types of fraud and the fraudster archetypes involved. But the challenge comes in dissecting and then piecing together who someone truly is and whether they are who they say they are. In the next chapter, we'll discuss the nuances of knowing your fraudster within the context of composed and synthetic identities and offer best practices to safeguard against identity fraud.

Q&A With Robert Reynolds

Q: Are there any people, businesses, or markets that you find are more likely to be targets of fraudsters? Does it vary by the type of fraud?

I think it tends to be concentric around where there's somewhat of a fungibility in the asset that they're stealing. So, lending is always a high-risk profile for fraud because the outcome is receiving cash, and cash is very easy to move and get away with.

There can be high-value, very fungible physical goods that are easy to move. And I think those are known as high fraud-risk items. A diamond necklace, for example. There are complications with that type of fraud that require the fraudster to have reshipping fraud as a part of their process, in terms of having a valid address to ship the item to and then ship it overseas or wherever the fraud is occurring.

So, physical fraud increases logistical complexity and improves failure rates. But it really is just a kind of basic economic calculation of what's the gross margin on the stolen identity that I have. Anywhere where that calculus becomes net positive, I think you're gonna find fraud. People are willing to take things for free regardless of how low value you may perceive them to be. Free is still free.

Q: Have you ever been surprised by a fraud?

Earlier in my career, I'd think of physical documents as being maybe fakeable but obvious when they are faked. And now I think that is wildly untrue.

Any physical documentation requirement upload—like a pay stub or a bank statement—to accomplish anything, there will always be a boatload of fraud in those environments. You can see really advanced methods of editing and/or finding valid formats for distributing that information.

When I was a little younger, I was very surprised to find the amount of effort that the fraudsters would and could put into making those documents appear to be pure and valid. And you know, you have companies like Pinwheel today that give you access to the source of truth information that makes it that much more difficult for frauds. You kind of take out the middleman. You're not uploading

documents; you're receiving them from the source. But on the other side of the equation, something that really, really surprised me was that fraudster ring that was extorting actual people to take loans out. You have these cohorts of consumers who are objectively good and show no fraud patterns. They have normal behavioral characteristics; they don't fit into any of the normal first-party fraud characterizations.

And you are just questioning: Why are there so many problems with this cohort of users?

When you figure out what's going on, it's somewhat terrifying. It's a movie scenario: someone with effectively a gun to their head, being told to do fraudulent things. That is happening in the real world, and it's very hard to stop.

Q: What are the most vulnerable processes fraudsters most frequently target?

They target physical documentation. They target humans as a point of weakness.

They will actively try and get pushed into call center operations or customer service agents to evade policies that are in place and try to reverse engineer them. And they are boisterous, and people fold under the pressure of someone being boisterous and maybe give them information that they shouldn't have.

I think humans are always the greatest point of failure—anywhere where human process is involved. And that tends to be like physical documentation in person or contact center interactions.

Fraudsters are becoming better and better, and the digital detection side of it is becoming more difficult.

Q: How do you see fraud continuing to evolve in the future?

I think the fraud prevention strategies that most people have available, and the types of data sources that most companies use to try and verify identities, have been relatively stagnant for quite a long time.

Outside of the behavioral characteristics, I have your email address that I can maybe verify the longevity of and the quality of. I have your phone number that I can verify the longevity and quality of, and I can even potentially call it.

But I think the prevention tactics become more well known, and people rely very heavily on those types of passive verification tools and things like device fingerprinting to stop large fraud rings. But the more well known the tools are, the more readily available ways to evade those tools become.

And I do personally worry that **the innovation on the prevention side is slower than the innovation on the attack side**. The tactics that currently exist are somewhat in terms of their effectiveness, and people need to start becoming a lot more invested in things like AI and machine learning to help really stop fraud in a more effective manner. Basic business logic is no longer going to cut it.

Q: Are there any mistakes or assumptions you commonly run into regarding fraudsters or fraud?

Organizations tend not to have dynamic enough policies in place to stop fraud. I think the fraud is going to adapt very quickly to the choices that you've made to prevent it, and you may feel great about the fact that you're preventing a known set of fraud, but I think it gives you a false sense of security. And I think for companies that I've worked for or worked with to try and help them build better strategies for fraud prevention, you find that they think fraud is more of a "set it and forget it" type of relationship. I think that is very disingenuous to the state of the ecosystem.

On a more tactical level, I've encountered companies that think that certain types of verification tools can be relied on very heavily, things like biometric authentication, or take a picture of yourself, take a picture of your driver's license. They think that it's not possible for fraud to exist in channels where those tools exist. And I think that is also like a fatal assumption to assume that any of your tools are perfect in their ability to prevent fraud.

Q: Tell us a little about the different types of fraud you encounter in digital environments.

Broadly speaking, everyone says first-party fraud and third-party fraud, but I think there's a lot more nuance to that.

There's ***true first-party fraud*** where the person has no intent to repay. In a lending environment, that's sometimes called friendly fraud as well.

There's also ***family fraud***, but it doesn't feel quite honest to place it next to true ID theft or actual fraud rings. Family fraud is when you have someone who is very close to the victim and can easily represent their identity, misrepresenting the state of their interest or needs. And that could be a spouse, caregiver, or another family member.

Then you have ***true third-party fraud***, obviously with ID theft. It can manifest either primarily digitally in the form of information gleaned from the dark web or stolen information from phising websites, but it can also manifest physically in the real world.

And I've actually had experience with this where we had fraud rings that were operating in different states in the United States. They were going to people and putting weapons to them and saying, "Apply for these loans, and we're going to take the proceeds and run away with them." So, it's, in some sense, first-party fraud because it was real information, but it truly was a third-party fraud ring that was manipulating first-party actors into committing the fraudulent deed.

And then, an entirely separate type of fraud, synthetic fraud, combines real and/or fabricated identity characteristics to effectively spoof the credit reporting agencies into creating "Frankenstein" identities. And that's a separate problem that is generally more resolvable through vendor relationships and/or data analysis.

Q: What is the most common type of fraudster seen in fraud prevention?

The most common that people quantify is third-party fraud because it tends to come with the strongest external dependent variable, which is people filing things like ID theft claims.

The things that go most underrepresented are likely first-party fraud. In a typical lending environment, they will often get rolled into normal delinquencies because it's very difficult to suss out the difference between credit risk, for example, and unwillingness to pay in the context of a loan environment.

Synthetic fraud is very difficult to identify purely because there is no one adversely affected by the fraud. There is no true identity that is kind of potentially exposed to loss, and the recourse of marking up someone's credit report is nothing when that person doesn't exist.

Q: Are there any atypical types of fraudster that you've encountered or that you see emerging?

You allow for normal good people to open accounts, take loans, whatever it may be in whatever the context of your business. And then, those individuals get phished, and fraudsters take over their accounts or manipulate call centers or operation centers to take negative action against those accounts.

I think there's definitely an uptick in that threat vector, primarily because a lot of the prevention methods tend to exist at the top of the funnel for businesses. So, once an account is open and the person seems to be good, it's tough to reevaluate that constantly, and it creates opportunity for fraud when the focus is elsewhere.

Q: Do you think companies have robust enough KYB/KYC policies? Why or why not?

Generally speaking, in my experience, if you take KYC as an example, the regulatory requirements for KYC are fairly broad: "Do you feel confident that you know the person who is applying for a loan?" The methods that companies use to satisfy their KYC requirements vary quite widely and, in my experience, tend to be somewhat derivative—or at least additive to actual fraud prevention methodologies.

How do you say that the person at you are looking at is not falling into any of the groups discussed above? The legal requirements are fairly thinly veiled in terms of whether you feel reasonably confident that you know who the person is and that this is the person who they say they are. The only way to really accomplish that is to layer multiple types of fraud strategies into place. You have to create a tiered approach, a layered approach, and a targeted approach to stop all these different kinds of fraud.

In the case of KYB, where you're verifying the legitimacy of a company or organization to assess the risk of doing business with them, that's more acutely associated with the actual legitimacy of the business. In that sense, just meeting the bare minimum of the legal requirement is not going to be nearly enough to actually prevent and mitigate fraud.

Q: What provides the most friction when companies create KYC/KYB policies?

I think the main friction point is that **if you want no fraud, you'll have no volume run through your business**. Where do you decide the right point of management is for acceptable risk tolerance, beyond meeting the KYC requirements? I think every business actively does meet those requirements. But if we're truly talking about fraud prevention above and beyond, the friction really exists. And how much friction do I want to introduce to my process to try and become incrementally savvier to fight against the different types of fraud? Managing those cutoffs and trying to get accurate dependent variables to model and/or evaluate against is very, very difficult.

What real fraud looks like can be very, very hard to determine. In the case of first-party fraud, how do I know someone is defrauding me? How do I know they had an unwillingness to repay? Creating a definition to surmise that is very hard because the person's not going to tell you, "Oh yeah, at the time that I applied for this, I had no intention to repay."

I think on the KYB side, it's largely that institutions are somewhat disincentivized from wanting to weed out potential clients or potential vendors. So, you have to create a system of true governance. One that can have the right kind of checks and balances in place to ensure that the motivations of individual employees to solve a specific problem are not the antithesis of what your KYB strategy needs to be successful.

Q: What do you think organizations most commonly get wrong about their KYC/KYB policies or strategies?

I think organizations on the KYC side don't put enough effort into evaluating. And I think this requires true human intervention, like evaluating and categorizing fraud into different categories and coming to good definitions. Like, this is what happened to this application or this consumer and putting them into those buckets: This was true third-party fraud; this was true first-party fraud. And being diligent about sampling enough of your consumer data to not just trust the definitions you have in place but staying vigilant and trying to observe new types of fraud.

Understand that you need to be constantly updating and changing your strategies to have a real, solid KYC strategy, especially when you're dealing with third-party fraud. You're effectively fighting against an enemy with unlimited time and unlimited resources. The idea that they're not going to change their strategies in response to your tactics is somewhat foolhardy. You need dedication to updating and changing.

I think KYB success relies very, very heavily on governance and process control to ensure compliance. Because the incentives of the business are not against the objectives of KYB, but they can be at odds with each other. People tend to want to get stuff done and get it done quickly. This type of governance to prevent fraud and make sure you don't get juked is just an additional process that people need to follow.

Q: Are there any behavioral characteristics that you think should be watched regarding how a fraudster would behave?

I think behavioral fraud prevention is easily one of the most effective forms of fraud prevention. I know what a good customer looks like, how they act, how much time they spend doing things, how often, and in which ways they communicate with me. And I think **one of the hardest things for fraudsters to determine is what that profile of a normal consumer looks like and to mirror it**.

So, when you look at event tracking or behavioral tracking and building models around it, the behavioral characteristics are some of the most indicative data sources that exist to mitigate some of the more advanced fraud tactics.

Q: Could you give me an example of one way in which a fraudster's behavior would differ from an ordinary user's?

They're going to spend just different amounts of time doing different things on your application or doing different things on your site. They're going to click their mouse in different ways. Typically, if they're a large third-party fraud ring that needs to automate the flow through your application process, their ability to create normal patterns of traffic for large amounts of volume is going to be relatively challenging—or can be challenging for certain types of fraud.

So, the locations of where they click on buttons or mouse movement, whether they tab through applications or prefill data, the types of devices they use, or the way they use those devices through the application processes, I consider all of those to be behavioral in a sense.

Kind of the sum of the parts is that you find clusters of users who tend to have behavior that is atypical. Those clusters of users tend to be related, and the relationship is usually fraud.

One of the cool things that I think more businesses should do is to not necessarily decline or weed out the fraud as early as possible. You identify it and just kind of let them do their thing, and then at the very last moment, you prevent it. That just allows you to acquire more behavioral information about the fraudsters themselves and use that for clustering or analytical purposes to identify future fraud with this same kind of risk profile.

Q: What do you think is the single most important thing a company can do to identify potential bad actors?

I think the most important thing is to be aware of the types of fraud that exist and put great, great, great concerted effort into things like manually vetting loans, accounts, and customers that have been a part of your system for a long time. Manually reviewing them and putting actual thought into it. Is this person actually good? Is this person actually bad? And why? Categorizing things in a way that gives you better data for analysis.

You can represent uncertainty in that data and evaluate against uncertainty; that's fine. But you have fraud, for example, that will open accounts and pay loans for nine straight months and then blow the account out, or open bank accounts and be a normal deposit user for a year and then wait for their moment and over-leverage the account.

And there are definite patterns in those accounts where you would look back and realize the stupidity of not noticing what they were doing previously. But I think it's because people tend to think, "If I don't have a problem at day zero, I'm going to be happy and not think more critically about this book of consumers that exist within my ecosystem."

You have to be very vigilant about putting human effort into analysis and critical thought—really evaluating things.

7. PricewaterhouseCoopers. "PwC's Global Economic Crime and Fraud Survey 2022." PwC, https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html.

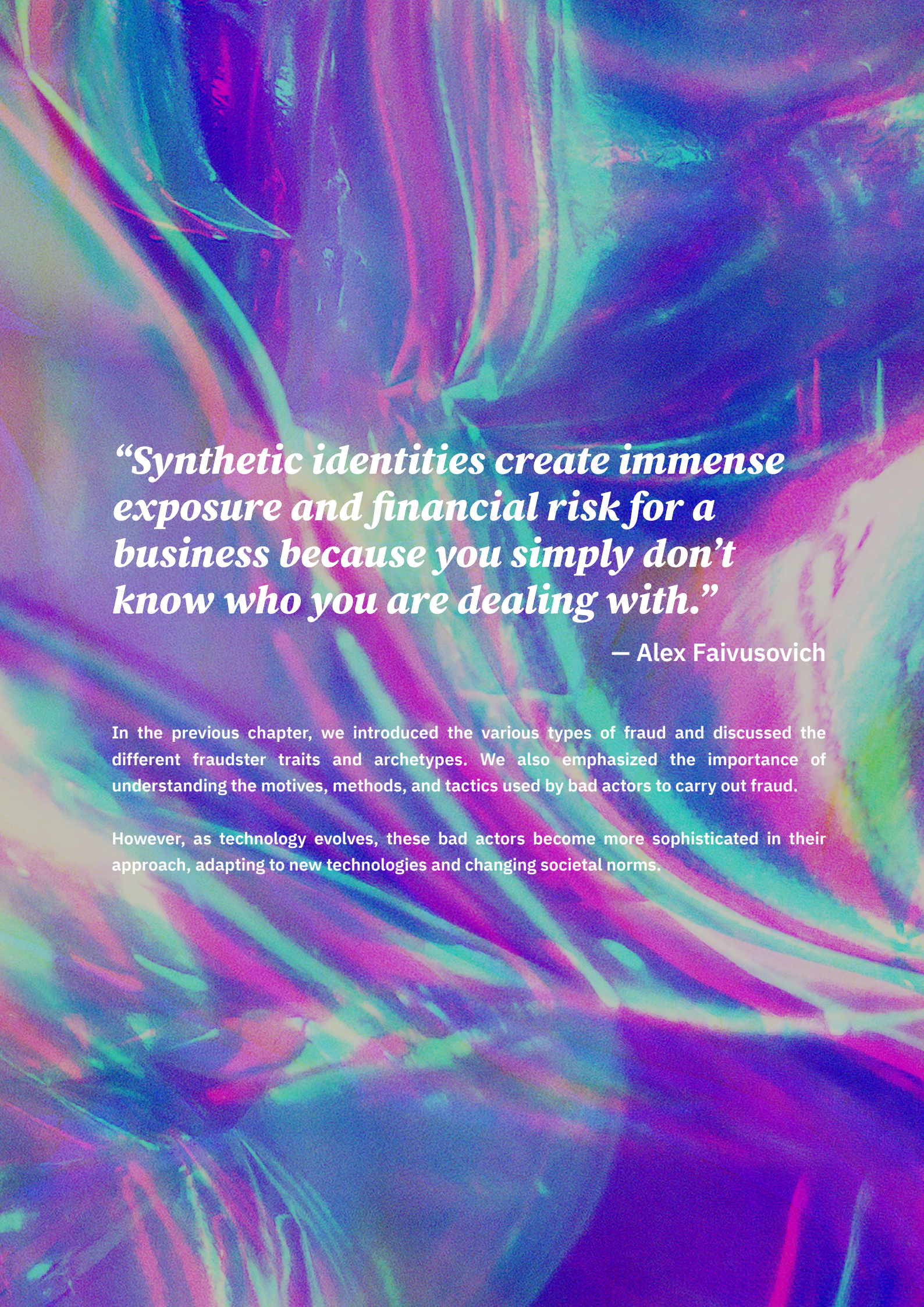
8. "7 Trends That Will Shape the Fraud and Identity Landscape in 2023" LexisNexis Risk Solutions, https://risk.lexisnexis.com/insights-resources/infographic/fraud-and-identity-trends.

9. PYMNTS.com. "Fintech Execs Expose the Real Costs of Fraud." PYMNTS.com, PYMNTS.com, 18 Nov. 2022, https://www.pymnts.com/money-mobility/2022/fintech-execs-expose-the-real-costs-of-fraud/.

10. PYMNTS.com. "The FinTech Fraud Ripple Effect - November 2022." Payments News & Mobile Payments Trends, Consumer Payments News, Financial Technology News, PYMNTS.com, 18 Nov. 2022, https://www.pymnts.com/study/fintech-fraud-ripple-effect-digital-wallets-instant-payments-money-mobility/.

11. Vedova, Holly, and The FTC Office of Technology. "New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021." Federal Trade Commission, 22 Feb. 2022, https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.


COMPROMISED
AND SYNTHETIC
IDENTITIES



“Synthetic identities create immense exposure and financial risk for a business because you simply don’t know who you are dealing with.”

— Alex Faivusovich

In the previous chapter, we introduced the various types of fraud and discussed the different fraudster traits and archetypes. We also emphasized the importance of understanding the motives, methods, and tactics used by bad actors to carry out fraud.

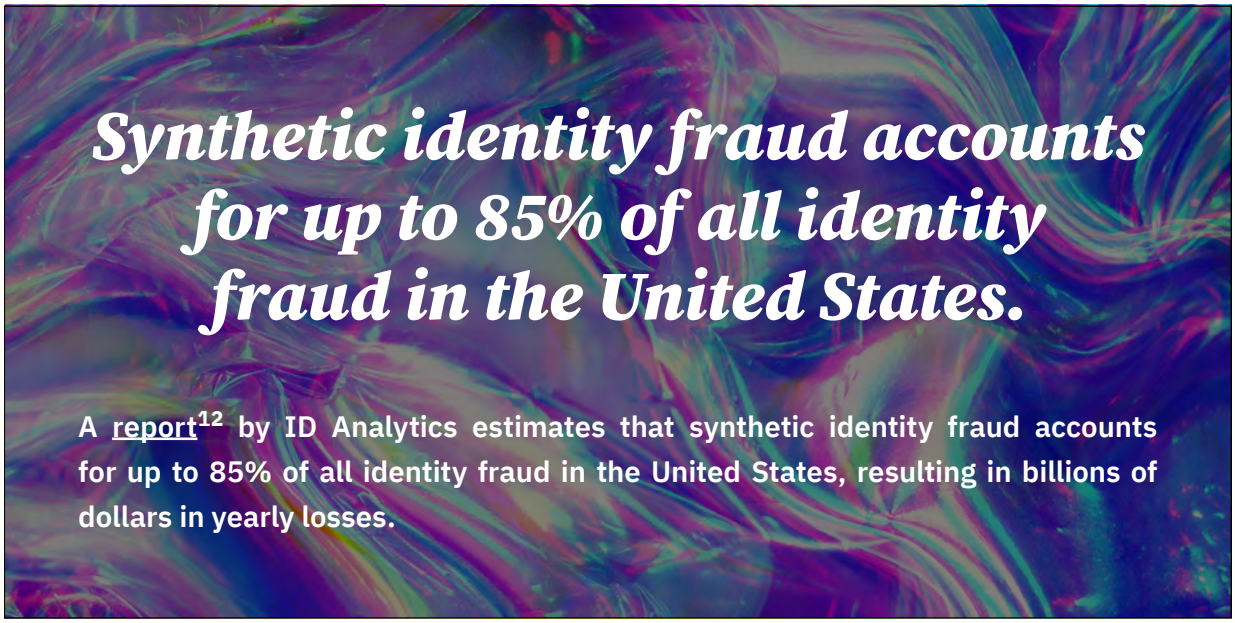
However, as technology evolves, these bad actors become more sophisticated in their approach, adapting to new technologies and changing societal norms.

In its earlier days, identity fraud involved stealing a person's identity information and using it without modification to open fraudulent bank accounts or get credit cards. But as financial institutions became more effective at discovering and preventing this type of fraud, bad actors learned to adapt and evolve.

One of the most significant developments in this arena is synthetic identities—new identities created using both legitimate and fake information. Because of this combination, synthetic identity theft is often harder to track and trace and is becoming increasingly popular amongst bad actors.

To gain more insight into the world of stolen and synthetic identities, how bad actors gain access to these identities through marketplaces, and the best practices for financial institutions and individuals to safeguard themselves against identity fraud, we interviewed Alex Faivusovich.

Alex Faivusovich is currently the Head of Fraud Risk at Unit21. Alex oversees the company's efforts to provide various organizations with advanced anti-money laundering (AML), fraud reporting, and Know Your Customer (KYC) compliance solutions. Alex brings over 15 years of experience in fraud prevention and investigation, and has led fraud risk operations and strategy in various Fortune 500 financial institutions and Fintech companies.



What Is Synthetic Identity Fraud?

Synthetic identity fraud is a type of fraudulent activity in which perpetrators use a combination of real and fabricated personal information to create a fictitious identity.

As Alex explains, “The fraudster will take elements of a real identity. For example, name and Social Security number, and add other elements like a false date of birth or phone number to create a new identity that does not correspond to any actual person.”

Once the bad actors create the synthetic identity, they can open fraudulent accounts, apply for loans or credit, and conduct other illicit activities. Synthetic IDs typically rely on a valid Social Security number (SSN), giving criminals the best chance at passing customer due diligence and KYC checks during onboarding.

Stolen vs. Synthetic Identity Fraud

Fraudsters use both stolen and synthetic identities with the purpose of committing fraud, but they go about it in slightly different ways.

In stolen identity fraud, “a real-life identity of someone is stolen,” Alex explains. A hacker steals all the elements of the victim’s personally identifiable information (PII), such as name, address, date of birth, and Social Security number.

With this information, the thief can open credit accounts, take out loans, and perform other nefarious actions while impersonating the victim.

Synthetic identity fraud differs from stolen identity fraud in that it involves the creation of a new identity rather than “entirely” using an existing one. In synthetic identity fraud, criminals use a combination of real and fake personal information to create a new identity that they can use to perform fraudulent activities.

Fabricated vs. Manipulated Synthetic Identities

Alex points out two types of synthetic identity—fabricated and manipulated. On the one hand, "a fabricated synthetic identity is made up of a variety of real and fake information," he says. For example, you take one person's name and another person's Social Security number and address and add a fake phone number and email to create an entirely new synthetic identity.

On the other hand, manipulated synthetic identities are usually created by taking an existing identity and modifying it to create a new identity. "So, for example, the bad actors will use their name, address, and phone number but will add a different Social Security number for themselves," Alex explains. He also adds that the most common reason for creating a manipulated synthetic identity is to bypass a bad credit history.

How Synthetic Identity Fraud Works

Bad actors can conduct synthetic identity fraud in many ways, but the primary method is, unfortunately, straightforward. "The only thing bad actors need to do is to come up with an identity combination that won't look suspicious," says Alex.

Here is a breakdown of how the process typically occurs:

1. Obtaining the Legitimate Information

A bad actor obtains an SSN and other personal information belonging to a real person, often by purchasing it on the dark web. Individuals with limited or non-existent credit history, such as children or young adults, are often easy targets for synthetic fraud. A paper by the Federal Reserve reports that over 1 million children[13] were victims of identity fraud in 2017 alone.

2. Creating the Synthetic Identity

At this stage, the fraudster combines some real identification (SSN) with false identifying information, such as a fabricated name, date of birth, and address, to create a synthetic identity that does not correspond to any actual person.

Alex points out that bad actors will often look to create synthetic IDs that won't raise red flags. "They try to make the synthetic identity appear as an applicant that a financial institution would like to work with," he says. For example, a middle-aged male living in a high-income neighborhood.

3. Integrating the Synthetic Identity Into the Financial System

Once the synthetic identity has been created, the bad actor's next step is to "input the synthetic identity into the financial system," Alex says. To do this, bad actors use the synthetic identity to apply for credit or other financial products, such as credit cards or loans.

The credit bureau typically declines this application because it cannot match the name of the synthetic identity in its records. However, applying for credit automatically creates a credit profile at the bureau in the name of the synthetic ID, so the fraudster can now set up accounts in this name and begin to build credit. "And this is how bad actors start the cooking process," Alex explains.

4. The Cooking Process

Because the credit bureau creates the synthetic identity file, the fraudster then begins building a credit history for that synthetic identity. As Alex describes it, the bad actors "add the synthetic identity as an authorized user on a credit card that they already have."

Over time, the synthetic identity builds up a credit history, making it easier for the fraudster to obtain more significant lines of credit or loans.

5. The Exit Scam

Once the bad actor has obtained access to significant credit or loan products, they may max out the accounts and then disappear, leaving the financial institution with unpaid debts and no way to locate the synthetic identity of the bad actor.

The long-term implications of synthetic identities.

"Some synthetic identities go all the way back to the late eighties and early nine-ties. So, we have thousands, tens of thousands, of synthetic identities in the market today cooked with 20, 25, 30 years of history," says Alex. "Bad actors can pretty much buy a house with a synthetic identity today."

The Effect of Synthetic Identity Fraud on Financial Institutions

One of the primary effects of synthetic identity fraud is financial loss. Alex further adds that "the real impact of stolen and synthetic identities is that it just creates such large exposure and financial risk for a business because you simply don't know who you are dealing with."

Synthetic identity fraud poses unique challenges for financial institutions because of the way the bad actors typically operate. Fraudsters use synthetic identities to establish credit and may act as excellent customers for months or even years before using the accounts for fraud.

Financial institutions may only detect fraud once the criminals have stolen significant amounts of money, which can take multiple missed payments or suspicious charge-backs. "The potential loss when you deal with either stolen or synthetic identities could be huge," Alex adds.

Synthetic identity fraud can also harm a financial institution's reputation. If a financial institution cannot detect or prevent synthetic identity fraud, its customers may see it as unreliable or untrustworthy. This can lead to losing customers and potential revenue, as well as increased scrutiny from regulators and the public.

How Fraudsters Gain Access to Sensitive Information

Bad actors use a variety of tactics to gain access to their victim's personal information. Some of the most common strategies include buying identities on dark and deep web marketplaces, implementing social engineering methods, and using deep fakes to bypass identity verification.

Deep Web Marketplaces and Communication Platforms Facilitate Sales of Stolen Identities

Deep web marketplaces like Genesis and communication platforms such as Telegram offer bad actors an easy way to buy the stolen digital identities they use for fraudulent activities.

Websites like Genesis[15] sit on the deep web, a website that is not indexed and can be accessed through traditional web browsers like Chrome or Safari. "All that is needed is a signup fee of like $100 worth of Bitcoin, and users gain access to the marketplace's offerings," Alex says.

This ease of access has made marketplaces like Genesis a popular choice for bad actors seeking to purchase personal information.

Cost of stolen identity on deep web marketplaces.

According to this VentureBeat article[16], a package of stolen identities on deep web marketplaces can cost anywhere between $0.70 and $350, depending on the type of data it contains.

High-end stolen identities usually contain more potent data, including users' previous purchase histories, active cookies, and login credentials, that give bad actors access to bank accounts or restricted company portals.

Platforms like Telegram and WeChat provide real-time communication encryption tools for these bad actors to interact and anonymously sell user information to each other. It also helps them communicate effortlessly with individuals and groups.

"Today, we have tens of thousands of Telegram groups that are dedicated to fraud, fraud as a service, as they call it," Alex says. "You can basically buy a fraud guide on a Telegram channel."

Social Engineering Attacks Culminate in Account Takeovers

Social engineering is a technique used by bad actors to manipulate individuals into divulging their personal information. The goal is to gain the target's trust and build rapport with them, often by posing as a trusted authority.

"Social engineering is about getting your target comfortable enough to give you their personal information. And it doesn't really matter what the tactic is," Alex explains.

By doing so, the bad actors can convince their victims to reveal sensitive information, such as email addresses, passwords, or Social Security numbers. Once these bad actors are in, they can use the victim's information to perform fraudulent activities.

Social engineering scams can culminate in account takeovers (more about this in Chapter 4) by giving cybercriminals access to sensitive information that they can use to gain unauthorized access to an account. And this affects both the individual and the financial institution.

"If a bad actor takes over one of your customers' accounts, it destroys their trust in your institution," Alex says.

Employees at financial institutions are also at risk. By performing seemingly unharmful actions such as visiting a website or clicking on an email, employees can unwittingly grant bad actors access to sensitive company information and data.

Deepfake Scams Blur the Lines Between Reality and Illusion

Bad actors also use AI and cloning tools to make fake images, videos, and voice recordings of real people—widely known as deep fakes.

Deep fakes are harmful in two ways. First, bad actors use them to bypass traditional onboarding processes and sign up on financial platforms, making it difficult for financial institutions to distinguish between legitimate and fake identities.

"One of the biggest weaknesses until recently with synthetic identities is that synthetic identities had no face. Now, with deep fakes, you can pretty much create a fake person, associate that AI-generated face with a synthetic identity, and suddenly the synthetic identity has a face," Alex says. "With that face, bad actors can even start applying for a state ID or driver's license."

The second issue with deep fakes is that bad actors use them for pretexting. Here, a bad actor poses as a trusted authority figure, such as a bank representative or executive, to trick the victim into revealing sensitive information or authorizing a transaction.

For instance, in early 2020, fraudsters used AI cloning and deep voice technology to swindle $35 million from a bank[17] in Hong Kong. The bank manager in Hong Kong received a call from a man he assumed was a director at a company with whom he'd spoken before. The fake director informed the manager that his company was about to make an acquisition, and he needed the bank to authorize transfers worth $35 million.

However, the manager didn't realize he'd been deceived as part of an elaborate scam in which fraudsters had used "deep voice" technology to clone the director's speech.

Such incidents are beginning to poke gaping holes in existing fraud operation processes as AI and deep fake technology continue to improve.

How To Detect and Prevent Synthetic Identity Fraud: 4 Best Practices for Financial Institutions

There is no silver bullet that can effectively combat all cases of synthetic identity fraud but there are a few effective steps businesses can take toward fraud prevention.

1. Understand Your Customers

The first thing Alex believes institutions fighting against synthetic identity fraud should do is drill down on their target customer profiles. “You want to be as accurate as you can be on your target audience,” Alex says. “Really understand the people who will organically want to adopt your platform, adopt your services, and sign up for your Fintech product.”

Understanding your customers is particularly important when designing onboarding systems. “Not every customer is willing to send you a copy of their ID, and not every customer is willing to take a photo or a selfie just to onboard your platform,” Alex points out.

You have to understand which population of your customers might be more accepting of friction and “be analytical about how and where you implement this friction” to onboard as many customers as you can, Alex adds.

2. Implement Robust KYC/KYB Workflows

As discussed in the previous chapter, the next step is implementing solid identity verification and Know Your Customer (KYC) and Know Your Business (KYB) strategies. These help your business detect and prevent unauthorized users from accessing data.

One of the ways to detect synthetic identities, Alex describes, is a process where financial institutions query customer data directly against the Social Security Administration (SSA) database instead of the credit bureaus. “You ask the SSA a simple question: does this combination of first name, last name, and Social Security number exist in your database?”

Alex adds that this process can introduce friction to the onboarding process and be expensive. “But it’s still one of the best ways of dealing with synthetic identity fraud today,” he explains.

3. Get All Employees Involved

Something we touch on in Chapter 6 is that fighting fraud should not be solely the responsibility of the risk department. “You need company-wide collaboration,” Alex says.

For example, the product manager who designed the product has to collaborate with the risk manager to understand where there might be security gaps in the product. In addition, the risk manager collaborates with the marketing manager to educate the customers on potential risks and how to prevent account takeovers.

The risk team should educate the customer support team to spot a bad actor or somebody who might be pretending to be someone else. “I think it’s a collaborative effort of a company to work together and ensure that you keep your customers safe,” explains Alex.

4. Implement System-wide Monitoring for Anomalies

One of the best ways to catch synthetic IDs is to monitor customer behavior for anomalies. You need a platform to aggregate data from different sources to get a holistic view of your customer behavior.

Monitoring your data systems goes beyond transaction or customer purchase data. You need all kinds of data together—personal information, transaction data, and risk insights you got from your KYC vendor.

The more data points you can bring in, the more sophisticated rules you can create to fight synthetic identity fraud.

Adopting a Collaborative Approach for Synthetic Identity Fraud Prevention

To conclude, Alex stresses the importance of financial institutions sharing information about synthetic identity fraud to help identify patterns and trends in fraud. Sharing information can help prevent fraudsters from moving on to the next Fintech company once caught by one company.

One idea that Alex mentioned is participation in a consortium database, where institutions can share information and work together to identify potential bad actors.

"This is something Unit21 offers our customers—a consortium database called the Fintech Fraud DAO that is fully dedicated to our customers," he explains.

"If Fintechs use a good consortium approach, they can utilize the data to be able to say, 'Hey, this person who tried to join your platform was flagged six months ago by a different Fintech company.' Then, the Fintech company would decide if they want to work with them or not."

Key Takeaways

- ***Synthetic identity fraud involves the creation of fake identities by combining real and fake information***
- ***The synthetic identity creation process can take months and years before the actual scam occurs***
- ***This type of fraud significantly impacts financial institutions by causing reputational damage, financial losses, and legal consequences***
- ***Fraudsters often gain access to sensitive information through data breaches, deep web marketplaces, and social engineering tactics***
- ***Best practices for detecting and preventing synthetic identity fraud include understanding your customers, implementing robust KYC/KYB strategies, leveraging fraud detection technologies, and adopting a collaborative approach***

As we've learned in this chapter, synthetic identity fraud involves the creation of a new identity using a combination of real and fake information. This identity can then be used to open bank accounts or apply for credit, which can be used to purchase things like cryptocurrency.

With the rise of blockchain technology and the proliferation of cryptocurrencies, bad actors are finding new ways to exploit vulnerabilities in the system. Chapter 3 will dive deeper into the world of cryptocurrency fraud, exploring the tactics used by cybercriminals and the measures that companies can take to protect themselves and their customers.

Q&A With Alex Faivusovich

Q: From your experience working in different industries, how would you say identity fraud has evolved over time?

First, we need to look at how fraud evolves. Fraud usually follows technology, so as technology evolves, fraud evolves. And if we apply this common sense to the financial industry, we can see how this plays out.

Let's say 30 to 40 years ago, if you wanted to open a bank account, you would have to go to a branch with your documents, provide your ID and proof of identity, sit in front of the teller, and have them verify that you are who you say you are. Then they will open an account for you. But in the early 2000s, when the financial industry moved into online and mobile banking, we lost the physical representation of identity.

So now, identity is only as it appears online. Whatever information you can gather online is your identity. There is no physical representation, body, or face.

This is where identity fraud started to ramp up, where bad actors understood that they no longer needed to go to a physical branch to open a new account. Instead, they can do everything online. And once you allow people to do certain activities online, fraudsters will always try to look for different ways to exploit the weaknesses that come with this newfound ease of use.

Q: What types of identity fraud are you seeing in the industry today?

Before diving specifically into identity fraud, I want to differentiate how we look at different types of fraud. So, when we say fraud, we say that it's an act of one person who deliberately tries to deceive another person or an organization for personal gain. And with that definition, we look at fraud from two different vectors.

The first is ***third-party fraud***, and the second is ***first-party fraud***. Third-party fraud is usually committed against an organization, but we don't know who's committing the fraud, meaning the person who's committing the fraud is outside of the organization.

On the other hand, first-party fraud is often committed by someone who misrepresents themself within the organization. So, it could be either a financial institution's customer or an employee, but this is somebody directly associated with the financial organization. And this is how we look at fraud: first party and third party.

Now, if we dive deeper into identity fraud, we have two different types of identity fraud—stolen and synthetic identities—and both of them represent different risks.

Q: What is the difference between a stolen and a synthetic identity?

A stolen identity is when the real-life identity of someone is stolen or used by a bad actor, hacker, or fraudster. The bad actor uses all the elements of the victim's personal identifying information (PII). Their first name, last name, address, phone number, email, and Social Security number—all those combined elements represent an actual person, a real person. And the bad actor steals that identity fully to use it illegally.

However, for synthetic identity, the fraudster will take elements of a real identity. For example, name and Social Security number, and add other elements like a false date of birth or phone number to create a new identity that does not correspond to any actual person. And with synthetic identity, we also have two types that we usually refer to—a fabricated synthetic Identity and a manipulated synthetic identity.

Q: What's the difference between fabricated and manipulated identities?

A fabricated synthetic identity is made up of a variety of real and fake information. For example, you take one person's name and another person's Social Security number and address and add a fake phone number and email to create an entirely new identity.

However, a manipulated synthetic identity involves modifying an existing identity to create a new one. So, for example, the bad actors will use their name, address, and phone number but will add a different Social Security number for themselves.

Q: Why would someone want to manipulate their identity?

It is usually done by people who have bad credit. For example, if I know I have a very low credit score but still want to lease a new car, I know nobody will lease a new car to me.

So, what can I do? I can create a synthetic identity under my identity and try to apply for a lease for the car, or I try to get a new credit card.

Q: Do you have any examples of stolen or synthetic identity fraud that you have dealt with in your career?

I think if I go back to the early days of the pandemic and back when I was working as Head of Fraud Operations at Lili Bank, we implemented monitoring dashboards to look for a combination of town and state and see how many applicants we have onboard from those combinations.

Two or three months into the pandemic, I was reviewing my alerts in the morning and saw a small town on the border of the United States and Canada—a really small town. And I had 39 new applicants from that town that morning, which didn't make sense.

Why would a small town on the border of Canada on one bright morning have so many people trying to onboard to my platform? When I started reviewing the KYC application, I saw that all 39 applicants came from two streets. And when I opened Google Maps, I could see that the two streets were parallel, and people from every house on that street were onboarding onto my bank.

Once I did some digging a few weeks later, I found out that bad actors hacked the town's website and accessed the portion of the website where people pay their water bills and local taxes on the properties. And that portion of the website contained the full identity of the homeowners. And what they did was use all those identities as stolen identities to onboard to the bank I was working for.

Q: How does identity fraud affect businesses?

I think the real impact of stolen and synthetic identities is that it just creates such large exposure and financial risk for a business because you simply don't know who you are dealing with.

If somebody applies to onboard on my Fintech platform with a stolen identity and they have a very high credit score, I might think, based on my internal underwriting models, that this applicant looks good on paper and want to give them a $50,000 credit line depending on what they want to purchase.

But I might not know that there is a bad actor who is operating that identity, and they have zero intention to pay. So, once the first payment doesn't come in, and then the second, I realize that it's a bad actor, and I'm liable to bear all the loss. The potential loss when you deal with either stolen or synthetic identities could be huge.

Q: How does this synthetic identity creation process work? Are there sophisticated technologies fraudsters use to create synthetic identities?

The method of creating a synthetic identity is, unfortunately, very simple. The only thing bad actors need to do is develop an identity combination that won't look suspicious.

First, they will use a common first name and last name. Next, they try to make the synthetic identity appear as an applicant that a financial institution would like to work with, (a middle-aged white male, for example). And they choose a date of birth representing somebody of middle age and an address that makes sense from a socio-economic perspective.

Once all that different PII information has been orchestrated and the synthetic identity has been created, they need to insert it into the bureaus. What bad actors do is they will go and apply for a small credit card, and the chances are they will get declined. But the biggest flaw with the way the bureaus operate is that even if they get denied, this synthetic identity is now registered at the bureau.

And what the bad actors can do now is add the synthetic identity as an authorized user on a credit card that they already have. And this is how bad actors start the cooking process. The cooking process of synthetic identity means they let this identity be in the financial market for a few months or years until it looks ready enough to go and execute large-scale fraud.

Q: How long does the synthetic identity fraud process take?

It depends on how big of a fraud they want to commit with this identity. Think about it: if I just created a synthetic identity, and three months later, I go to a Mercedes dealership and try to buy a $200,000 Mercedes, chances are the dealer will look at me and say, oh, you have a credit history of only three months. I'm not sure I want to sell this car to you.

But if I'm patient and I wait five years, I keep adding this synthetic identity to more credit cards. Now I have a $100,000 worth of credit line associated with this identity, and I never missed a payment, and the credit score suddenly looks like 790 or 800. If I go back to the Mercedes dealership and show them, "Hey man, I'm good. I pay all my bills on time. I have a great credit line. Sell me the car." Chances are they will sell me the car.

And synthetic identities are not new. Some synthetic identities go all the way back to the late eighties and early nineties. So, we have thousands of synthetic identities in the market today cooked with 20, 25, or even 30 years of history. Bad actors can pretty much buy a house with a synthetic identity today.

Q: How do bad actors get access to customer information?

Today, data breaches are still the number one cause of stolen identities. It could be a data breach on a municipal or town hall website, a hospital, fast food chain, or big retail store like Target or Walmart. If those businesses get hacked, and the bad actors are in the database, they extract all the customer data and then sell it. **Data breaches are the number one cause of identity fraud today.**

Q: What types of information do bad actors steal?

You need to think about it from the bad actor's perspective. The people who do data breaches and sell information on the dark web are usually not the same people who perform identity fraud. It's like different jobs in the market. Some people sell, and some people buy.

If I'm a bad actor and bought your identity today, I will try to go after you and take everything you have. I will try to send you phishing emails and hack your social media. I will try to access all your bank accounts. I will try to take over any account I can because now you are my asset.

And the more I can get out from you, the greater damage I can cause. So, if I have your Social Security number, full name, date of birth, and address, I will apply for credit cards. I can get 100, 200, and 300 thousand dollars worth of credit lines if you have a good credit history and buy a car with your identity, but it doesn't end there.

If I hack your social media, now I can go and send messages to all your friends on social media and all your contacts and try to get money from them by telling them—"Hey guys, I'm stuck in Mexico with no money. Send me money."

Now I'm using you as an asset, and I attacked all your friends. I can also hack your health insurance account and medical records. And if I see you are suffering from a type of disease, I can try to blackmail you and say, "If you don't pay me $100,000, I will tell everybody that you're sick."

So, the victim is exposed in so many ways beyond the financial damage. The bad actor can cause damage to their reputation and to their friends. And this is what we see today. A bad actor that gets a victim's information will try to get the max out of it.

Q: What's the role of deep web marketplaces like Genesis and communication platforms like Telegram in synthetic identity fraud? Why are fraudsters migrating to these platforms?

With Genesis Market and many others like Genesis Market, you need to understand how things are shifting in the fraud market. So, if we go back, let's say 10 years ago, if you wanted to buy a stolen identity, like a compromised credit card, you probably needed to go to a dark web marketplace or join a forum to show some credibility. Then you will get access to those databases.

But most people, especially if they're not hackers, don't know how to access the darknet. They don't know what a TOR browser or onion address is. They don't have the technical capabilities to access darknet marketplaces. And the operators of those darknet marketplaces understood that they needed a different way to bring the product to the people because of demand.

And that's where marketplaces like Genesis were born. So, Genesis sits on a deep web. A deep web is a website that is not indexed, and you can access it from your regular safari or Chrome web browser. And all that is needed is a signup fee of like $100 worth of Bitcoin, and users gain access to the marketplace's offerings, which is why it became so popular.

Telegram is a fairly encrypted platform. So, bad actors can operate fairly anonymously on Telegram without being caught or spotted. And today, we have tens of thousands of Telegram groups that are dedicated

to fraud—fraud as a service—as they call it. You can basically buy a fraud guide on a Telegram channel; books will teach you how to commit fraud. So, all this became much more accessible to the general public.

Q: Why can't platforms like Genesis be stopped or shut down by law enforcement?

Who's responsible for shutting them down? Is it the US government? Or the European Association? Or African entities? Or Telegram? So, no one person is responsible? If you shut one down, they will open a new one. So, is there even a point in playing this cat-and-mouse game?

Q: How can businesses, especially financial institutions, implement measures to detect and prevent fraudulent transactions related to illegal marketplaces?

One of the things financial institutions can do is hire cyber security companies that have access to all those marketplaces. And then, tell them to search the marketplaces and bring a list of identities they find. So, when the bad actor tries to use those identities, they can block them from onboarding.

Q: Does artificial intelligence have a part to play in social engineering attacks?

I think the biggest abuse of AI today is not necessarily correlated with identity fraud, but it's more correlated with social engineering scams. How can I use AI today to make you feel comfortable talking to me?

We are seeing new reports of how people abuse voice AI. Are you familiar with a situation where you get a phone call, but nobody talks on the other side? You get a call, and it's quiet for about 20 seconds, and then the other party hangs up.

What bad actors do is record your voice, and now that they have a sample of your voice, they can feed it into the AI or the machine learning algorithm and call your mother with your voice saying, "Hey, I'm, I'm stuck somewhere. Can you send me $10,000?"

And then we have the issue of deep fakes.

Q: How do fraudsters use deep fake technology to commit identity fraud?

One of the biggest weaknesses until recently with synthetic identities is that synthetic identities had no face. Now, with deep fakes, you can pretty much create a fake person, associate that AI-generated face with a synthetic identity, and suddenly the synthetic identity has a face. With that face, bad actors can even start applying for a state ID or driver's license.

Q: Do you have any examples of how deep fakes can affect financial institutions?

One of my hypotheses on deep fakes is that bad actors will use job openings to pose as fake employees. So, for example, let's say a bad actor wants to penetrate a bank or a company. They can look for a job opening in finance, and since most interviews are now done by phone or Zoom, they can bypass those with a deep fake technology to onboard a company, and now they can access the company and customers' financial accounts and potentially steal funds.

Q: Is there a new way financial institutions can protect themselves from deep fakes?

Most document and face verification algorithms today know how to detect deep fakes. But then again, deep fake technology gets better and better every day. So, it's like a chess game. But we are not far from the point where a human eye won't be able to detect if a particular video is a real person or an AI-generated person.

However, as deep fakes develop, we will also have tools that will help us to predict if an image, video, or voice is AI-generated. There are a few companies like Microsoft and Google that are helping develop these tools.

Q: What are the most significant challenges that financial institutions face when it comes to preventing identity fraud?

The biggest challenge in fighting identity fraud today is understanding where and how to create friction. For example, we spoke briefly about document verification and face recognition.

However, you cannot do it for every customer because not every customer is willing to send you a copy of their ID, and not every customer is willing to take a photo or a selfie just to onboard your platform.

So, financial institutions have to understand which population is more vulnerable, which might be more accepting of friction, and be analytical about how and where you implement this friction to achieve balance.

Q: Do you have processes financial institutions can look for to determine if an identity is stolen or synthetic?

With stolen identities, we try to understand the correlations between what we see from the applicant and what we expect from the applicant. For example, let's say we have an applicant who is using the stolen identity of someone from California, but he tried to onboard on our platform from a mobile phone, which the IP tracks back to New York. We would ask ourselves why a person whose address is in California would try to onboard to our platform from New York. Then we will look for other pieces of information to check the identity—for example—if the email or phone number correlates to the identity.

Synthetic identity is different because we try to look at the various elements of the identity, not who uses it, because we already believe it's not a real person.

We try to understand whether or not this identity exists in real life. **One of the ways to detect synthetic identities is to query not against the credit bureaus but directly to the Social Security Administration.** You ask the SSA a simple question: does this combination of first name, last name, and Social Security number exist in your database?

This is the solution for detecting synthetic identities today. Does it have friction? Yes. Is it expensive? Yes. Do you need consent from the applicant? Yes, but it's still one of the best ways of dealing with synthetic identity fraud today.

Q: Looking ahead, what are the biggest identity fraud threats, and how do you think the financial industry will evolve to tackle these emerging threats in the future?

We're seeing now that bad actors understand that it's much easier for them to execute fraud on Fintech platforms because Fintech platforms, compared to more traditional brick-and-mortar banks, tend to be less strict and more accepting of different users and different identities. And I don't see this trend stopping soon.

Taking a consortium approach is the key to success in the next several years. Everybody talks about fraud evolving, but before fraud evolves, it's shifting. So, it'll be in this Fintech today. And once they understand they can no longer do it with this Fintech, bad actors will jump to another Fintech.

If Fintechs use a good consortium approach, they can utilize the consortium data to be able to say, "Hey, this person who tried to join your platform was flagged six months ago by a different Fintech company." Then the Fintech company would decide whether they want to work with them or not.

And this is something that Unit21 offers our customers. We have a consortium database that is fully dedicated to our customers, Fintech companies.

Q: What role does a company like Unit21 play in combating identity fraud?

The most significant feature of Unit21 is we help companies unlock all the different data silos they have. For example, financial institutions might be working with various KYC vendors and getting customer data from multiple sources, but if they don't have a place to aggregate all the various data points and look at them holistically, it's tough to fight fraud.

And this is what Unit21 unlocks for our customers. We bring companies' data silos into a unified system to help them gain visibility and implement processes and rules to fight fraud.

When you only look at transactions, you're only considering financial data. That alone might not give insight into identity fraud. However, if you start incorporating additional data elements like KYC information, PII, applicant origin, device type, IP geolocation, and other relevant factors, you can develop a more sophisticated fraud prevention strategy.

The other part is our consortium product. We allow companies to take a sneak peek at what happened with an identity in another Fintech company and make decisions based on that.

Q: How can a new Fintech company ensure its onboarding process is secure from identity fraud?

If you are starting a Fintech company today, first, **you want to be as accurate as you can be on your target audience and really understand the people who will organically want to adopt your platform, adopt your services, and sign up for your Fintech product. This will help you understand where and how to create friction in your onboarding process** and the parameters to check for to differentiate between a real or a synthetic identity.

The next thing is you need company-wide collaboration when you're fighting fraud. Fraud fighting is not only with the risk department. The product manager who designed the product has to collaborate with the risk manager to understand where there might be security gaps in the product. The risk manager collaborates with the marketing manager to educate the customers on potential risks and how to prevent account takeovers.

So, I think it's a collaborative effort of a company to work together and ensure that you keep your customers safe.

Q: What final advice would you give individuals and businesses to protect themselves from identity fraud?

My advice for individuals is to keep their passwords sophisticated and 2FA everything. It's worth the extra 10 to 15 seconds it'll take you to log into your account. You are much more protected if you use 2FA.

The second piece of advice is to be extremely cautious when interacting online with strangers. **If a stranger approaches you with an offer that sounds too good to be true, then it is probably too good to be true.**

For businesses, keep your data safe. Unfortunately, we have seen data breaches take place almost daily. So, you are obligated to your customers to keep their data safe, do everything in your power, and use all the tools, cyber companies, and features to protect your data. Because if a bad actor takes over one of your customers' accounts, it destroys their trust in your institution. And once you lose the trust of your customers, they will no longer do business with you.

12. The Changing Face of Identity Theft - Federal Trade Commission. https://www.ftc.gov/sites/default/files/documents/public_comments/credit-report-freezes-534030-00033/534030-00033.pdf.

13. "Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors." FedPayments Improvement.org, The Federal Reserve, July 2019, https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf.

14. "Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors." FedPayments Improvement.org, The Federal Reserve, July 2019, https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf.

15. Lyngaas, Sean. "'Operation Cookie Monster': FBI Seizes Popular Cybercrime Forum Used for Large-Scale Identity Theft | CNN Politics." CNN, Cable News Network, 5 Apr. 2023, https://www.cnn.com/2023/04/04/politics/genesis-market-fbi-seizure/index.html.

16. Staff, VB. "Netacea: Stolen Identity Sales in Criminal Marketplace up 250% since 2019." VentureBeat, VentureBeat, 23 Apr. 2021, https://venturebeat.com/business/stolen-identities-sold-in-criminal-marketplace-soared-250-since-2019/.

17. Brewster, Thomas. "Fraudsters Cloned Company Director's Voice in $35 Million Bank Heist, Police Find." Forbes, Forbes Magazine, 9 Nov. 2022, https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=49548d0b7559.


CRYPTO
CURRENCY
FRAUD

“Anybody, whether a high school kid or a criminal, can use cryptocurrency to transfer assets and value anywhere in the world.”

— Kevin Yang, Nibiru

It may seem as though every month brings another high-profile “crypto fraud,” from malware attacks fueled by cryptocurrency to large-scale cryptocurrency exchanges getting shut down.

It’s estimated that $14 billion in value was lost to crypto scammers in 2021[18]: a record-breaking number. As people become increasingly familiar with and adopt cryptocurrency, more fraudsters start to use it to their advantage.

In the first half of 2022, the Department of Justice charged a handful of cryptocurrency cases—valued at $2 billion[19]. Cryptocurrency fraud isn’t just a matter of volume but raw scale: it’s not just that more fraud is occurring; it’s that very large volumes of currency can be stolen simultaneously.

In this chapter, we discuss cryptocurrency fraud, why it happens, and how to avoid it with our expert Kevin Yang, the Core Engineer and co-founder at Nibiru. Nibiru is an integrated ecosystem of products including Nibiru Chain, a new crypto derivatives protocol that makes it possible to stake, swap, provide liquidity, and trade futures on the blockchain.

Why Does Crypto Attract Fraudsters?

Cryptocurrency has many of the advantages of cash: it is difficult to trace and easy to distribute. Today's fraudsters can commit digital crimes on a global scale, digitally launder their funds, and transfer them into a local currency—sometimes within mere minutes.

For individuals, the risk is simple: they can have their cryptocurrency stolen from them by a fraudster or be tricked into investing in a fraudulent cryptocurrency scheme. Two common types of cryptocurrency schemes are "pump and dumps" and Ponzi schemes.

Pump and dumps: Crypto creators boost their currency's price artificially (often through raw marketing) and then cash out, causing the price to plummet on other investors.

Ponzi schemes: Crypto creators use new investments to pay out old investments, building the illusion of a stable cryptocurrency, but it is actually not profitable.

Organizations that manage cryptocurrency have a different set of risks. While they also could be taken in by pump and dumps or Ponzi schemes, their concerns primarily relate to the cryptocurrency they manage.

Money laundering: Fraudsters can use middlemen to launder their cryptocurrency; organizations must verify that the funds are legitimate.

Compromise: Fraudsters can steal money directly from an organization—and if the organization's wallets are compromised, it may not be possible to get the cryptocurrency back.

In short, cryptocurrency doesn't attract any new types of fraud—but it's highly attractive because it has the benefits of cash (such as being difficult to trace) alongside the benefits of digital currency (such as being easy to transfer).

"The point of blockchains and cryptocurrency is to have an open, decentralized, no-nonsense network for transferring assets," says Kevin. "Anybody, whether a high school kid or a criminal, can use cryptocurrency to transfer assets and value anywhere in the world."

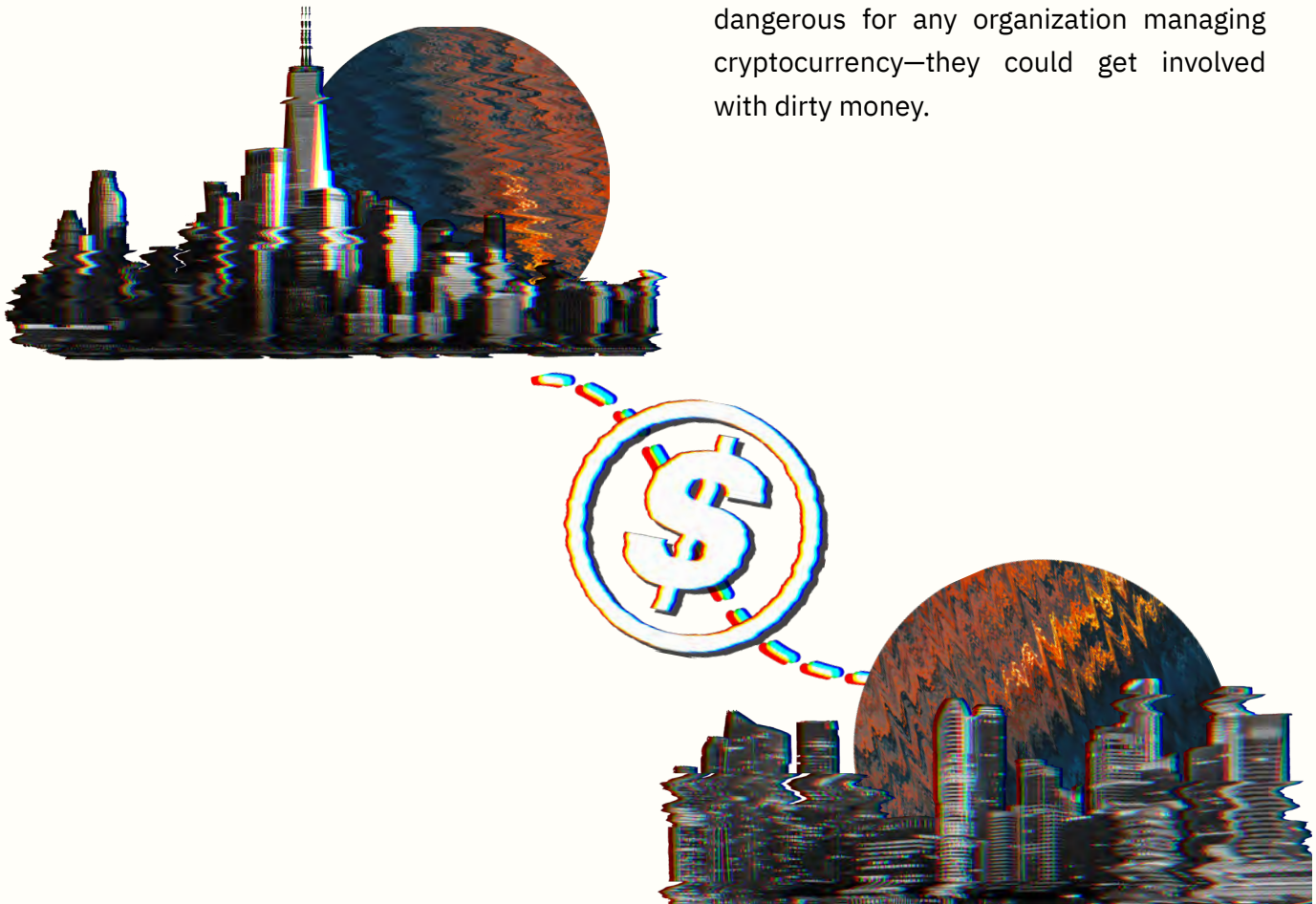
Money Mules of the Modern Age

Organizations must be particularly wary of money mules—individuals using a platform as a way to move funds. This cryptocurrency may be involved in large-scale crimes: ransomware attacks or even terrorism.

"I can send some money to somebody in Singapore right now," says Kevin. "It'll take a few minutes to receive. I would even argue that, in certain places, depending on the type and the nature of the criminal we're dealing with, there's no need for cash bills anymore."

Crypto makes it easy for people to take money anywhere. It's a digital currency, but it can live in a physical space; you can take a million dollars in Bitcoin onto a plane in a USB drive without alerting the authorities. And you don't even need to do that: you can transfer millions across the internet in a single transaction (or millions of transactions).

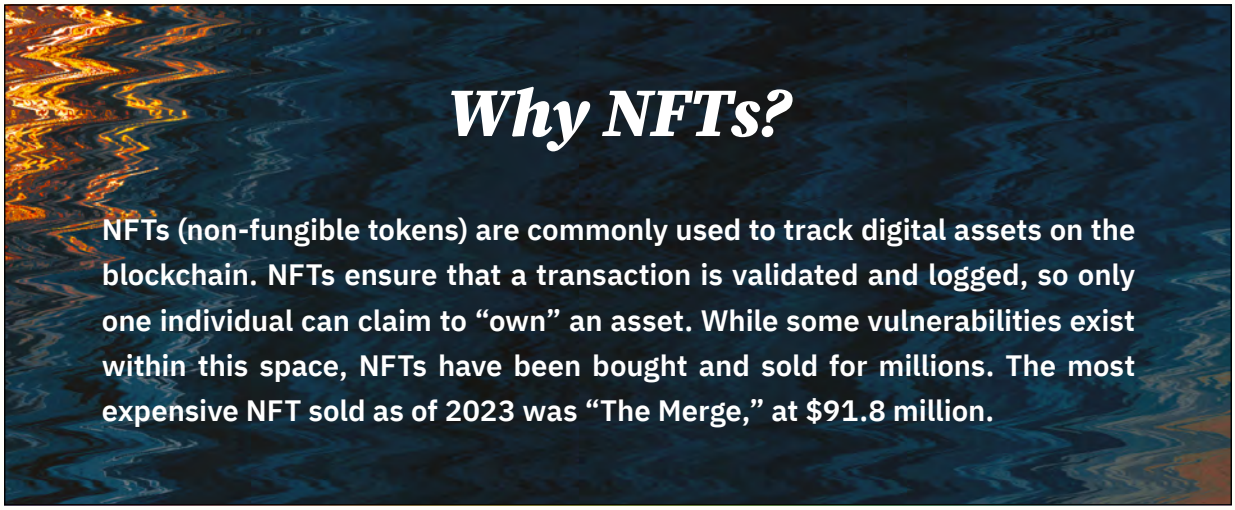
Money related to crimes can be laundered through money mules. Not only does this make it particularly difficult to track, but it's dangerous for any organization managing cryptocurrency—they could get involved with dirty money.



Web3, the Metaverse, and NFTs

As Web3, the metaverse, and NFTs grow in popularity, cryptocurrency fraud will only become more commonplace and complex. Web3 and the metaverse make it more likely that individuals will start to adopt cryptocurrencies—and as they live their lives online, they become more likely to invest in NFTs.

People are already living increasingly digital lives and purchasing digital assets, much like they might purchase downloadable content in a video game. Today, individuals can purchase digital real estate in the metaverse, tracked through NFTs.



Why NFTs?

NFTs (non-fungible tokens) are commonly used to track digital assets on the blockchain. NFTs ensure that a transaction is validated and logged, so only one individual can claim to "own" an asset. While some vulnerabilities exist within this space, NFTs have been bought and sold for millions. The most expensive NFT sold as of 2023 was "The Merge," at $91.8 million.

As more value is held within these technologies, more fraudsters will also become interested in the market. Kevin envisions a world in which people are completely anonymous, presenting themselves with synthetic digital identities and conducting crimes with ease.

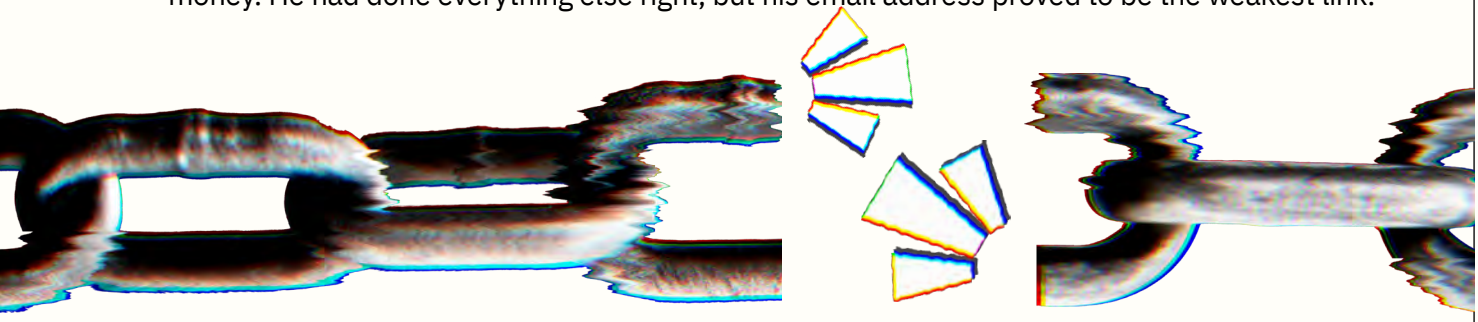
"There are tools in Web3 that make it so that your transactions are private," says Kevin. "It doesn't even show which address is sending transactions—or how much you're sending."

While these transactions are primarily relegated to early adopters today, they will likely become more mainstream with time.

Digital Assets—and How To Protect Them

Although there are few things as "digital" as cryptocurrency, the best way to protect cryptocurrencies (and other crypto assets, such as NFTs) is through physical security measures—cold storage. Other measures include real-time, on-chain monitoring, and system redundancy.

Kevin tells a story: his friend had everything secured through an encrypted key, but the encrypted key was connected to his email address. His email address was compromised; he lost a lot of money. He had done everything else right, but his email address proved to be the weakest link.



Cold storage: Digital information may be attacked from anywhere because the attack surface is broad. Cold storage (physical storage disconnected from the internet) limits this attack surface. Physical wallets and USB keys are the least likely to be compromised.

On-chain monitoring: Similar to network security, real-time on-chain monitoring (the monitoring of transactions as they occur) can help organizations detect fraudulent transactions before their effects cascade.

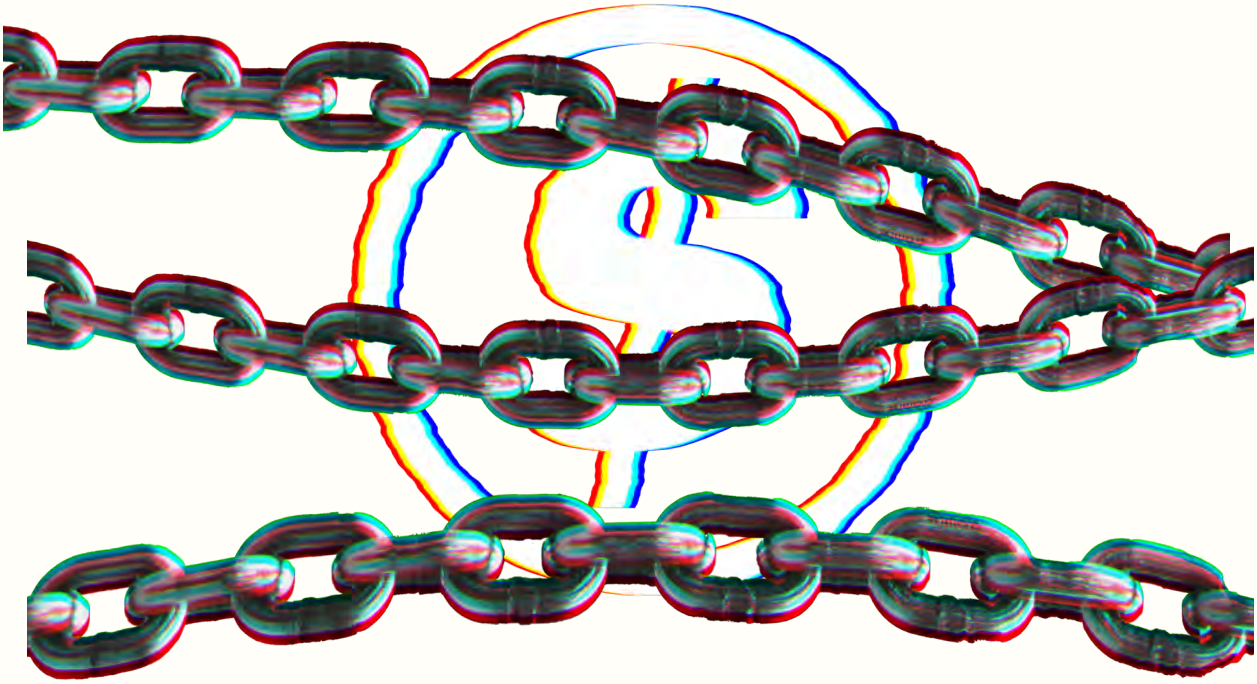
Redundancy: Organizations need to understand the underlying technology and take action to protect it. Cryptocurrency runs through peer-to-peer and community-run solutions; in other words, the organization isn't fully in control of its own infrastructure. It relies on these community servers and nodes. If the organization hasn't built up its own infrastructure and provided for redundancy, the whole system could be taken down.

Further, individuals should never share their information—and should be skeptical about who they trust with their digital assets. Organizations must thoroughly vet vendors and cryptocurrency technologies, gauging not only the tech but the people behind the tech.

Kevin points out that you can have, for instance, a very slick platform but no one interacting with the community—or when they do interact, it seems obvious they are just out for cash.

Kevin explains, "There's no company that runs the blockchain; it's people who set up mirrors or validators. These endpoints or services get attacked by malicious people who want to prevent others from using the network, or they have some financial opportunity to gain from doing so."

Regulating the Digital Frontier



Until fairly recently, organizations have been left to their own devices to figure out how they want to control and manage crypto assets. But regulations are likely to increase within the next few years, both in terms of how crypto is managed and how crypto-related assets and income are reported.

"The SEC and the IRS are getting smarter about tracking data on chains," says Kevin. "And so they'll probably get better at catching tax evasion, etc. Before, it was kind of lawless; they didn't really know what was going on with crypto, and you could just report the cost basis and short-term gains or losses however you wanted."

Increasing regulation is on the horizon—and some regulations have already been implemented. Cryptocurrency may soon be treated like a traditional currency, which also means that organizations will become more responsible for not only the money they hold but where it has come from. Specifically, the IRS has moved toward the accurate reporting of cryptocurrency and will hold organizations and individuals liable for gains made through crypto trading.

While this does mean that organizations need to be more cautious and skeptical regarding their cryptocurrency dealings, it also paves the way for safer, more secure, and more widespread adoption.

Summary

Although cryptocurrency fraud seems to be particularly prevalent now, at least some of it has to do with the growing pains of an industry with little regulation. Other elements that can lead to fraud—such as the growing mainstream adoption/ease of use of cryptocurrency and its lack of traceability—are actually overall benefits of the technology.

As the technology matures, it will become far safer. Organizations can protect themselves by following general best practices, including KYC/KYB—which we talked about in an earlier chapter. By knowing the individuals and businesses that they engage with, organizations can reduce the risk of encountering fraudsters and dirty money.

Key Takeaways

1. ***Cryptocurrency is on the rise both because it is becoming more popular and because it's difficult to trace***

2. ***Increasing regulations will likely make the market more stable, although increased adoption may also increase fraud***

3. ***Organizations should protect themselves with robust KYC/KYB policies by thoroughly vetting cryptocurrency partners and by engaging in on-chain transaction monitoring***

In this chapter, we learned that fraudsters use phishing or other means to steal login credentials and gain unauthorized access to a user's cryptocurrency wallet or exchange account in crypto fraud. After obtaining access, they can transfer the victim's cryptocurrency to their own accounts, which is usually difficult or impossible to recover.

Similarly, account takeover fraud also involves an attacker gaining unauthorized access to a user's account using phishing or other tactics. They use the account to carry out fraudulent transactions, transfer funds to their own accounts, or steal sensitive information.

In the upcoming chapter, we'll delve deeper into account takeovers, which is another type of fraud that is now widespread and increasing.

Q&A With Kevin Yang

Q: Why do you think crypto fraud is on the rise?

There are a lot of reasons here. Cryptocurrency makes it easy for anybody to transfer digital assets without having to prove their identity. The point of blockchains and cryptocurrency is to have an open, decentralized, no-nonsense network for transferring assets. That was the original intention of Bitcoin. Anybody, whether a high school kid or a criminal, can use cryptocurrency to transfer assets and value anywhere in the world.

We see this general adoption—more and more people are using it[20]. Compounding this is that there are so many new tokens and methods of transferring value. Before, like a long time ago, when cryptocurrencies and the web were new, we had Bitcoin and Ethereum. Now we have thousands upon thousands of assets. So, it becomes easier to hide your tracks or cover it up by bouncing across all these different currencies.

Q: How are organizations most frequently targeted by crypto fraud?

I think one of the biggest ones is phishing. Getting an email that sounds like it's from somebody else in an attempt to compromise confidential information, like your private key for your crypto wallet. Once you get the private key, that pretty much unlocks all the funds in your wallet. You can have phishing emails and you can have fake websites that look like real websites.

The other way that companies get attacked, and we've experienced this too, is that a lot of cryptocurrencies right now run on community infrastructure. There's no company that runs the blockchain; it's people who set up mirrors and validators. These endpoints or services get attacked by malicious people who want to prevent others from using the network, or they have some financial gain from doing so.

Q: Are there known profiles or archetypes of cryptocurrency scammers?

Anybody can do it. You don't have to go to the bank with your ID and open a bank account to transfer money. You can just connect. All you need is an internet connection, and you can connect to a blockchain network like Ethereum and start sending money. And without that identification process, you remain anonymous. There are tools in Web3 that make it so your transactions are private. It doesn't even show which address is sending transactions—or how much you're sending.

So, these tools actually make it really easy for people to get away with money or launder money. There's no centralization aspect. If your credit card gets stolen, you can report it to Visa or Mastercard, and they can cancel that credit card and possibly refund some money. There are safety features in place, and that's possible. We have governing entities that take care of those types of procedures. But in crypto and Web3, there's nothing like that.

There are no repercussions; it's kind of like a lawless land. It's like the Wild West right now because people can get attacked by somebody on the other end of the world with no jurisdiction, law enforcement, or extradition. That makes it a playing ground for fraudsters.

Q: How does fraud differ from NFT vs. traditional cryptocurrencies?

There are many types of fraud. There are "pump and dump" schemes where people will boost up the perceived value of an NFT art collection by claiming that it will give you access to some sort of benefit, social status, or tangible access, like clubs around the world. And then, once you buy the NFT, other people buy the NFT, and the NFT collection gets sold. The people who created the NFT can just run away with the money, and the value of the NFT gets diluted.

With NFTs, it's more vibe-driven. I mean, there are smart contract codes to write NFT projects that aren't complicated. There have been open-source

examples of it. But a lot of it has to do with marketing and social media content that's basically hyping up the NFT. I think it has a different target audience than people who try to commit fraud with decentralized finance and cryptocurrencies.

Q: What about money mules? Are there money muling scams that don't contain obvious red flags?

So, money mules: I would define it as somebody who carries money from point A to point B. For example, the head of a cartel wants to smuggle money across borders. They would hire money mules and take advantage of how everyone has a limit of how much cash they can bring across borders, take advantage of that kind of dead money over there.

With cryptocurrency, it's a lot easier—all your assets live on a chain. You just need to know the private key to build those funds. If I want to send money to a person and know where he is, I just need to send the private keys somehow, and that could be via a hardware wallet. Because the asset's digital, you don't have hard cash, which can trigger authorities and show up in scanners. You can have just a little USB drive, and it becomes a lot harder to detect.

Even simpler than that, you can send assets on the chain without going through a middleman. So, you don't have to wire money from a bank or go through Western Union or ACH transfer to somebody. You can send it right on the blockchain, and they'll receive it. I can send some money to somebody in Singapore right now. It'll take a few minutes to receive. I would even argue that, in certain places, depending on the type, the nature of the criminal we're dealing with, there's no need for cash bills anymore.

Q: What kind of crypto regulation do you think we will see become law, and will be enforced in the next few years/next decade?

The SEC and the IRS are getting smarter about tracking data on chains, and so they'll probably get better at catching tax evasion, etc. Before, it was kind of lawless; they didn't really know what was going on with crypto, and you could just report the cost basis and short-term gains or losses however you wanted. But the IRS is getting a lot smarter at that.

And there will probably be a lot more scrutiny around stablecoins in the future because there was a stablecoin last year called USDT which crashed; it went from billions of market cap to almost zero within a few days. There was a bank run, and they didn't have enough capital to cover a shortfall. That caused a lot of market losses for a lot of people and hurt investors. I think we will see a lot more scrutiny of stablecoin and centralized exchanges. They'll need to report their finances and conduct audits.

Globally, I think China is going to continue to be very anti-crypto. I think the United States is still trying to figure it out. Nobody knows for sure because there's a lot of internal debate about the utility of cryptocurrency and its value to society, the philosophy, and the power struggle.

Q: What do you think the cryptocurrency community needs to do to be ready for increased regulation?

More audits, more security, and playing by the rules. Crypto had a bad reputation for several years because of all the scams and frauds. If you will be operating in the United States, you must comply with the SEC reporting rules. You have to operate like an exchange. If you're operating in the United States, you must operate like you're governed by US rules.

One thing you could do right away is to implement a KYC process. If you want to use a decentralized application, you must upload identification or a utility bill proving you're not a criminal or terrorist. That helps with money monitoring because you can identify the customer and users.

And security audits. One of the big reasons people are scared of crypto right now is all the hacks going on. Smart contracts are code written by humans, and humans are imperfect. So, having an extra pair of eyes from white hat hackers or security firms to make sure there's no division by zero error, buffer overflow error, or just improper logic can help users feel secure and probably get a stamp of approval from the government in the future.

Q: How can people and organizations protect their crypto assets?

The absolute hard rule of crypto-currency wallets is never to share your mnemonic or private key with anybody. Private keys are just a series of text and decimal numbers. Those are very hard to remember and write down. So, people have created basically an algorithm to take a string of 12 or 24 words that are easy to remember: that's your mnemonic. But it's unique to you; common words like zoo, animal, or laptop. That can be turned into your private key. So, your mnemonic and your private key are equivalent, and they are of paramount importance.

Another thing you can do is use something called a multi-sig wallet. To send a transaction to the blockchain network and dispense the fund, you need a threshold of people to sign the transaction. So, instead of having one person own it, you can have three, five, or nine. So, you'd need at least three, five, or nine people to approve a transaction. You can have a democratic consensus.

So, that's a good way to protect highly valuable assets. Hardware wallets (cold storage) are another technology. Basically, instead of having all your private keys exist on your computer or in the cloud, they exist on a handheld device—kind of like a USB drive. It has additional hardware encryption modules on top of it, so basically, every time you want to send a transaction, you need to connect your hardware wallet.

Even if your laptop or cloud gets compromised, your hardware wallet will change your private keys, so it's safe. **It's better to never, ever store private keys on the internet, even if it's encrypted. Because you never know.** Let's say you use iCloud or send it to yourself in an email, and you have perfect protection, but someone's in the same public cafe as you and just hanging on the network. It's not impossible for them to intercept your messages and listen to your packets.

Another example: a friend of mine had his encrypted keys in an email to himself, but his email got hacked, and he lost a lot of his NFTs last year. So, the more physical you can keep your mnemonic and private key, the safer it is.

Q: What can organizations do to keep scammers from using their sites and engaging in crypto scams?

So, one thing you can do is watch your data—because all the data's public and available. You can detect things like the age of accounts. If it's an actual person's account and they use cryptocurrencies regularly, you'll see histories of transactions and applications they've interacted with.

Attackers will just use a script to create new accounts. These accounts are like bots on Twitter; the age of the account is a day or a week old, and they have no history at all and zero followers. You can do something similar on blockchains, so that would be something to watch out for.

If some projects or applications are being launched, but the owners are staying anonymous, that's a red flag to watch out for. It makes it easier for them to run away with the money. They might get caught later, but they might be in some jurisdiction with no extradition. You can't catch them, right?

Security firms will always display the projects they've audited before—you can see which projects these firms have audited that have been hacked and if there's a history of these products getting hacked. If a security firm audited such a project, they're probably not great security auditors. A lack of security audit or a security audit by a not-so-great security firm is another flag to watch out for.

A lot of cryptocurrency projects have a community built around them. You have Discord and Twitter, and you can see how legit they are and how much they actually care about people. If you hop on Discord and see the type of culture there is—if there's just a bunch of people who just care about the token launch—it might just be another rug-pull project or a get-rich-

quick scheme. But if they're dead set on the project's utility and want to make the world a better place, I know it sounds cliche, but that's a good sign.

Q: Can you see automation or AI changing things in the future?

Automation, definitely. Botnets fall under the category of automation. You are automating user traffic to these different points. AI is an interesting one. There are so many possibilities there, especially with the release of ChatGPT.

With AI, you can have AI write code. AI can audit your smart contract code and tell you the obvious flaws. One of the most popular programming languages used to write smart contracts is Solidity. It's not a difficult language to pick up, but it's easy to shoot yourself in the foot if you're not careful.

It works both ways. As a programmer, you can use it to detect flaws in your code and fix them as a hacker or attacker. Because all smart contract code is public, you can feed smart contract code through the AI bot, and it will tell you where all the vulnerabilities are.

Going further down the sci-fi path, you can even have chatbots pose as real people in Discord or on social media to make a project seem legitimate. You're no longer interacting with this seemingly degenerate person who doesn't care and only wants to get rich, but an AI bot who is programmed to be empathetic and talk to you in a customer support type of way.

If your AI is powerful enough, you can feed it all the blockchain data and kind of use it to catch obvious behaviors of money launderers. One thing money launderers would do is they would obtain a large pile of cash and divide it into small chunks, sending pennies or dollars to other accounts they own. You'd get this scatter effect from the accounts, and it becomes hard for a human to trace. But a bot could read through that and determine whether the behavior is suspicious.

It's kind of a cat-mouse game; if there's something you think the good guys can use AI for, the bad guys can use it, too. You have an intellectual warfare right now between the good and bad.

Q: Are there any common misconceptions about cryptocurrency fraud that you'd like cleared up?

There are many very polarizing people working in cryptocurrency; people who are smart and eccentric and people who are bad and immoral. It kind of happened that it's possible for one bad apple to spoil the whole bunch.

It's easy to generalize and say that everything you don't understand has to be a scam or that cryptocurrency is bad, but there are a lot of good ideas. People have these intentions to make the world a better place or more efficient, such as giving access to financial products or banking services in countries that don't have access.

When the Russia-Ukraine war started, citizens were able to escape with their life savings because of blockchain. In countries where inflation is high, like Venezuela, cryptocurrencies offer a stable currency for people to transact with. And the transaction fees and the transaction processing time are a lot faster than other networks in areas where the banking infrastructure is weak. You can have a settlement within seconds or minutes rather than having to wait a couple of days.

So, there are a lot of good ideas. I'm not saying that all of them are right or will work. But there are many really innovative people and a desire to do good in this space.

18. Sigalos, MacKenzie. "Crypto Scammers Took a Record $14 Billion in 2021." CNBC, CNBC, 7 Jan. 2022, https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html.

19. "Crypto Enforcement." The United States Department of Justice, 27 Feb. 2023, https://www.justice.gov/criminal-fraud/crypto-enforcement.

20. "Crypto adoption among retail and institutional investors in 2022" Finoa, Cryptocurrency Adoption and Growth: Statistics for 2022, https://www.finoa.io/blog/crypto-adoption-growth/.


ACCOUNT
TAKE
OVER

"The sad fact is that everybody's at risk. Ensuring that customers are protected is an ongoing concern for basically everyone in the industry."

— Kenny Grimes, Mercury

In addition to fraudster types, identity fraud, and crypto fraud, another form of fraud that's growing fast is Account Takeover (ATO). According to the Q3 2022 Digital Trust & Safety Index by Sift, ATO grew 131% YoY from 2021 to 2022[21]. But there are ways to detect ATO attempts and red flags you can look out for to keep you, your employees, and your users safe from this type of fraud. For this chapter, we spoke to two experts: Kenny Grimes and Tanya Corder.

Kenny Grimes is the Head of Strategy & Analytics at Mercury, a banking platform for startups of all sizes. With a career focused on managing risk and improving operational processes in tech, Kenny has seen the evolution of Fintech fraud over the past several years and has useful insights to share about ATO prevention.

Tanya Corder is a compliance manager at Treasury Prime, a platform that powers Fintech organizations by providing tools to build financial services ecosystems fast. Tanya has over 10 years of experience in financial services and compliance, providing insight into suspicious activity and financial fraud.

What Is Account Takeover?

ATO is a type of fraud that occurs when a bad actor gains access to someone else's account or personal information, often for financial gain. It can happen with any kind of online account but most commonly affects social media, banking, and eCommerce sites. Bad actors are using technology to script attacks using bots. For example, they have a massive database with a combination of credentials and mass-test them across a platform.

What makes ATO particularly tricky, Kenny points out, is finding the culprits of this form of fraud. "It's extremely difficult to pinpoint where it's happening and who's doing it," Kenny says. "It's highly efficient."

The information required to conduct an ATO is most commonly acquired through phishing, malware, data breaches, brute force attacks, or even public information.

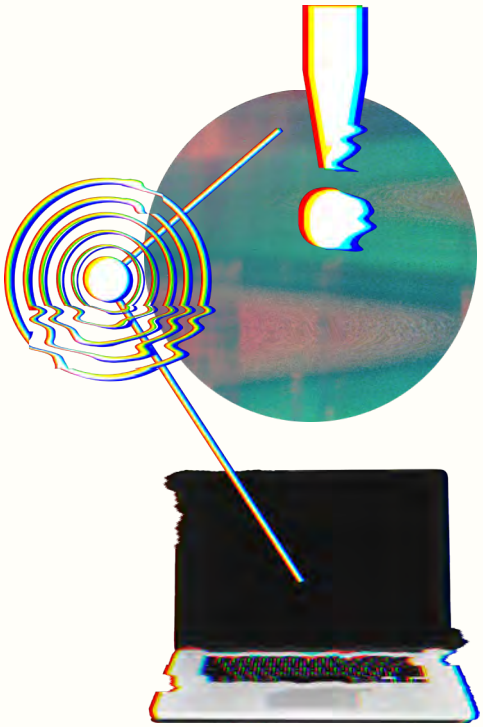
The 4 Stages of ATO

An account takeover doesn't happen all at once; instead, it starts small and progresses. Sophisticated fraudsters will be more difficult to detect as they know how to be stealthy and cover their tracks. There are four steps to a typical account takeover. The fraudster first gathers information on the account, then gains access and makes small changes before finally taking off with the user's hard-earned money.

1. Information Gathering

This stage is largely invisible. The fraudsters are working behind the scenes using whatever information is available. Tanya points out that fraudsters will "gather information about their target email addresses, phone numbers, and social media profiles."

This stage can be considerable, in terms of both time and effort, especially for fraudsters working to take over business accounts.



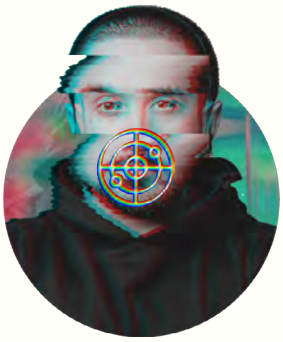
2. Account Access

Fraudsters often log in and make sure they can really get into the accounts before initiating any big changes. Many individuals and organizations often won't notice this stage.

"Fraudsters can use victims' accounts in ways that appear normal and can get away with things for sometimes prolonged times," Tanya says. "It makes it difficult for victims to notice that their account has been compromised because the activity looks so normal."

Organizations with any kind of online account feature need to be on the lookout for suspicious account activity that suggests this stage of ATO, Kenny says. “So, you’ll see a new login from an IP or location that has never logged into that account before.”

There might be other minor signs: you might see many failed login attempts across multiple accounts on your platform, or you might notice accounts that don’t usually log in often are doing so multiple times a day. But the fraudster hasn’t yet made a big move. If users are getting unexpected password reset prompts or other unusual activity, that’s a sign that there may be fraudsters trying to access accounts.



3. Small Account Changes

Once bad actors know they can access the account, they will often make smaller changes to set up their fraud or cover their tracks. Unless the user on this account is on the lookout for any suspicious activity, this step is easy to miss. “Usually, they’ll change login details or add their own contact information,” Tanya says. For example, fraudsters might quietly add a new person to the account or open new accounts altogether. They might also switch off notification settings so that their changes will go undetected for longer.

It’s important for the platform to keep an eye out for an increase in complaints or strange account behavior that could point toward fraud, Tanya says. “If there’s an increase in customer complaints about unauthorized access or fraudulent activity, it might be a sign that an account takeover is occurring on the platform. If there are multiple instances on the platform, it may be a sign that there’s a vulnerability in the system that is being exploited by fraudsters.”

4. The Money Grab

The final stage is when many people realize something is wrong after the damage has been done. New lines of credit may appear, money might vanish, or the user may be locked out of their own account entirely.

At this stage, the victim has to play catch up to figure out what happened and how the fraudster pulled it off. The process of attempting to recover the funds is difficult and time-consuming, and it's often impossible to recover everything lost. That's why it's essential to spot fraudsters before they reach this stage.

When bad actors attack your identity, they are not only after your bank account; they are after everything. They want to know where you buy your prescriptions so they can leverage health issues against you. They want to understand your full travel history so they can mimic you.

They will hack your social media along with your gym and any forums you belong to; this will give them access to more targets that usually interact with you on various platforms.

Who Is at Risk and Why

"The sad fact is that everybody's at risk," Kenny says. "There's almost no way to entirely avoid it."

Tanya agrees. "Anyone (and everyone) is at risk for account takeover. Specifically, anyone who uses an online account or engages in eCommerce in any capacity is vulnerable." That said, individuals and organizations most at risk are:

Populations inexperienced with technology

They're more likely to have poor security hygiene (like using the same password repeatedly), and they're less likely to know the signs of common forms of online fraud (for instance, suspicious emails phishing for sensitive information).

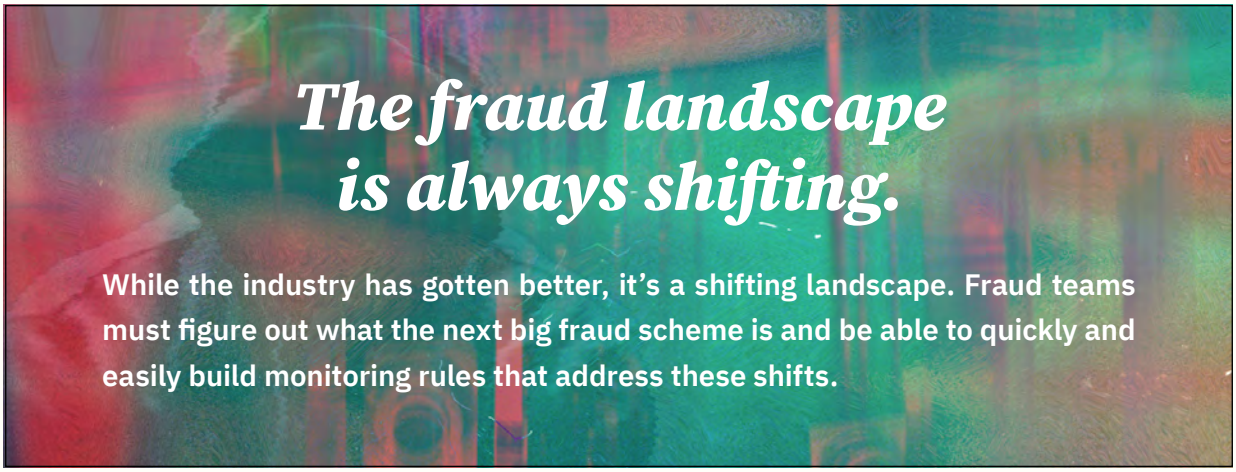
Small businesses

Startups and small businesses often don't have the resources to invest in sophisticated security tools or hire dedicated security roles. This lack of resources makes business email compromise an even bigger threat for small businesses.

High-profile individuals or organizations

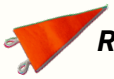
Because there's simply more information (like birthdays) about people and organizations available to the public, there are more opportunities for fraudsters to collect information. "High-profile individuals who are well-known celebrities or public figures, they're also at higher risk for takeovers," Tanya says, "because their personal information is more widely available, so their accounts are more attractive targets for fraudsters."

Both experts stress that no matter how sophisticated and thorough an organization's processes are for handling and protecting accounts, there's always a possibility that ATO could happen. In the same way that security features advance and individuals learn about how to protect themselves from fraudsters, fraudsters continue to develop new schemes to gain access to accounts.

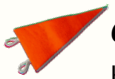


ATO Red Flags

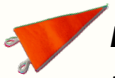
In order to protect your users and your platform, it's important to be aware of signs that ATO may be happening. Look out for these red flags:



Repeated attempts of 2FA: If a user has attempted 2FA several times in a matter of minutes or seconds, it could be a malicious attempt to gain access to an account.



Changes in login patterns: There might be logins from unusual locations or more logins than usual. Any significant change in the patterns of a single user or multiple users could be a sign that fraudsters are gaining access to the account.



Disabled security features that were previously enabled: They might turn notifications off so the victim won't be alerted when the fraudster makes changes to the account.

Deleted emails or other missing information: To cover their tracks, Kenny says, fraudsters attempting an ATO might send emails and receive emails from your accounts: "They'll even send messages and then delete them from that person's inbox right away and try to capture the responses before they can get them," he explains, to "basically set up a scenario where they're trying to get you to pay funds into an account by sending a fake invoice that's modeled after communications they've seen within that invoice."

Small, unexplained purchases or withdrawals: This can be a test before larger sums are taken out. If any accounts experience a series of small, unexplained purchases, that could be a fraudster preparing for bigger heists.

Keep an eye out for anything out of the ordinary, and if anything seems like a red flag, act immediately.

How To Prevent ATO

Kenny says it's important to remember that ATO is often preventable if organizations and individuals are aware of the ways account takeovers happen and are consistently looking for ways to identify and prevent these instances before they happen.

- Double-check any ***unexpected purchases or invoices*** with vendors by calling them on the phone instead of relying on email.

- Stay on the lookout for any ***unusual account activity***, especially the red flags listed above.

- Promote the ***one door, one key approach***. Never use the same password for two different accounts.

- ***Change passwords regularly*** on your accounts and encourage any users or customers to do the same.

- ***Use a password manager*** for yourself and your organization to make generating and storing passwords simpler and more secure. "The benefit, the value that a password manager has that I think a lot of people overlook, is that it recognizes where you've logged in successfully before," Kenny says.

- ***Enable 2FA*** wherever possible.

Key Takeaways

- ***ATO is a type of fraud where a bad actor gains access to someone else's account or personal information, often for financial gain***
- ***ATO has four stages: information gathering, account access, small account changes, and the money grab***
- ***Red flags of ATO include repeated attempts of 2FA, changes in login patterns, disabled security features, deleted emails, and small, unexplained purchases or withdrawals***
- ***To prevent ATO, double-check unexpected purchases, stay on the lookout for unusual account activity, use a password manager, change passwords regularly, and enable 2FA wherever possible***

Anyone with an online account is at risk of account takeover fraud.

Despite the perceived inconveniences, individuals must take a level of responsibility for following security hygiene best practices like using a password manager and implementing 2FA where possible to keep themselves and others safe from being taken advantage of.

However, the organizations that collect and store customer information are also at risk of data breaches and can be held liable for damages associated with poor fraud prevention practices, which is why it is critical for these companies to understand how to use security tools effectively.

To help with this, Chapter 5 will dive into the basics of fraud detection and prevention. We'll cover the different types of fraud detection solutions, transaction monitoring and risk assessment best practices, and adopting a dynamic approach.

Q&A With Kenny Grimes

Q: Why is ATO such a popular form of fraud?

Fintech fraud has changed over the last several years, at least since I've been in the industry. When I first started in Fintech, it was these single-point attacks and just trying to get funds through—single-actor-type things. But recently, in the last three or four years, it's become essentially a fraud marketplace, and it's a very highly optimized landscape as far as how fraud is committed across these accounts.

For example, an initial group of fraudsters will steal a bunch of IDs and then sell them on a marketplace-like dark web exchange. And then, another group of fraudsters will buy those stolen IDs to open a bunch of accounts which are then later sold on a marketplace. Those open accounts can then be used in any number of fraud scenarios ranging from an exit path for wire fraud, a sleeper account for ACH and check fraud, or a way to move other stolen funds across the financial system.

So, what complicates that from a risk perspective is that it's near impossible to identify who's committing the fraud because it's not just one person. It's extremely difficult to pinpoint where it's happening and who's doing it. It's highly efficient. People specialize in their area and can do it at a much greater scale. Rather than having a handful of accounts be attacked, you have these big waves of attacks all at one time.

ATO fraud tends to follow a similar wave trend where when fraudsters identify an ATO vulnerability, they'll try to impact as many accounts as possible while the vulnerability exists and can be done by several fraudsters in parallel.

Q: How rampant is ATO right now?

It's an ongoing concern. Mercury has a security team dedicated to solving this problem and making sure that our customers are protected. So, it's a concern for all financial institutions and making sure that investments are made there; otherwise, customers are at risk. Ensuring that customers are protected is an ongoing concern for basically everyone in the industry.

Q: Who is most at risk for an ATO?

The sad fact is that everybody's at risk. There's almost no way to entirely avoid it. However, those with worse security hygiene are going to be more at risk. And when we say security hygiene, it's ensuring that you don't use the same passwords across multiple accounts, having 2FA on your accounts, and using a password manager. Those types of things help prevent account takeover. The more of the good security hygiene you do, the less at risk you are for ATO. But getting to zero is quite challenging, as these fraudsters are quite innovative at times.

Q: And how do they go about getting this information?

The common classic one is brute force attacks, where someone is essentially aware of a good login. This person has an account with this institution, and I know their email address, so just guessing passwords. That's less common now because 2FA is a lot more common than it used to be. There's been a Twitter compromise in the last five years, so if your Facebook password or Twitter password is the same as your bank account, someone can go get that list of passwords and then use it to get into your account. Again, 2FA kind of gets around that as a benefit.

But compromised email is another thing. If your actual email user password gets taken over and your bank's 2FA is sending an email to you to verify our code, it kind of gets around it, right?

The more common things that are happening now are phishing attacks. So, getting an email for, "Hey, your statement's ready." And it's a click login to an account, which looks very much like your banking account, but it's not. That's someone gathering your username and password, as well as sending you the 2FA prompt that you then need to log in. When you enter your 2FA, it'll seem like you didn't log in; it'll be weird and feel like a bug. But what you just did is you authorized a new browser session for a fraudster. Someone has a valid session into your account, and then they can do what they want.

Also, cloned login pages, in general, can be a risk. There's a common attack if you're a known institution. To illustrate the example, I'll use a fictitious bank, let's call it Unicorn Bank. Many consumers will go to Google to log into Unicorn; you type in Unicorn Bank, and on Google, that top link to Unicorn Bank is often an advertisement and might not really be Unicorn. So, fraudsters might buy a similar-looking domain like unicornonlinebanking.com, maybe slightly misspelled because of the available domains. And then you click on that one, it looks like a Unicorn bank account, you click through, and it's actually not a Unicorn page. You're logging into a clone page, and someone's getting your username, password, and 2FA. Those are the modern scams.

And then a final classic one is customer service social engineering—knowing that someone has an account somewhere, calling up and trying to get access, like, "Oh, I can't log into my account, please help me."

Q: Are there predictable stages for account turnover?

If we think about this from the perspective of the platform or the institution where the account is logged into or where the account is being held, there are several actions that will happen.

You'll see a new login from an IP or location that has never logged into that account before. Oftentimes that's the standard, "Oh, we should 2FA that device. It's a whole new device we've never seen before." However, on the cloned pages where you're giving someone's user password and then you're entering that 2FA, you'll see a login from a brand-new device that you've never seen before. It'll 2FA, and they'll get a valid session. But then you'll see within usually 30 seconds to a minute another login from a known device. Having a fast fall login for the same user from a known device is usually the pattern that triggers the platform to flag that this might be an account takeover scenario.

As an institution: **Know that that's the pattern and have appropriate alerting on it**. Do additional security checks with that application, have them reviewed by your security staff, or restrict additional functionality. You can't remove funds without doing an additional 2FA, like adding an additional friction down the line, to protect funds in the account when that may have happened.

Another red flag for this is repeated 2FA. Multiple failed login attempts across multiple users from the same IP are a sign of it as well. As far as the consumer viewpoint of it, the red flag you usually get is 2FAs that you don't recognize. So, it's like, "Did you log into the account?" That's usually the sign that someone knows their account may have an issue. Or getting the alert that a transaction is pending. Having noisy alerts when transactions happen to validate that those transactions should be happening. And so those alerts become critical to give someone at least time to validate whether or not that's a payment that they wanted to make.

Q: Is there anything an individual or organization can do to prevent these issues from happening under their nose?

My top recommendation is always to use a password manager. And you might think, "Oh, use a password manager so that you can use a unique password with every login." This is a benefit, and you should totally do it and use stronger passwords and not know what your passwords are. The other value that a password manager has that I think a lot of people overlook, is that it recognizes where you've logged in successfully before to that specific domain.

So, if you're on one of those spoof login pages and it looks like your Chase login, and it's not prompting you to enter in the password from your password manager, that should trigger something in your mind: Hey, do I trust this login page? Because the password manager's used to seeing unicornbank.com/login as the login page, and that's not what this website is. It might be U-N-I-I-C-O-R-N, a misspelled uniicorn.com/login, which is not a valid login page.

That becomes an additional layer of security of having something check that you're on the right website before entering a username and password. That will help prevent phishing attacks. That'll help against spoof login pages, as well as having all the additional security hygiene of good, randomized passwords.

On the business account side, a lot of times, you have your admin account to log into the account, but then your accounting department also has logins to your account to get access to it. You have multiple entry points into this account, and you must also trust the password hygiene of all those other users.

At Mercury, we take 2FA a step further. We use device verification so that when you try to login to a new device – even if your password and 2FA is correct – we require you to validate your new device via email. In addition, we also support Security Keys (like TouchID), which are extremely resilient to phishing.

One thing we've built at Mercury is secondary approvals on certain transaction types. For every wire at ACH, any user of the account has to be approved by another user. So if, for whatever reason, your Mercury account just got past your security and that person wants to wire out $100,000, the fact that it needs another approval makes the funds much, much more secure.

Q: What are the differences in ATO when it happens to individuals versus entire organizations?

One thing that organizations deal with that individuals typically don't is a concept called ***business email compromise fraud***. It's a type of account takeover where it's not necessarily your account being taken over; it's one of your vendors' email accounts getting taken over.

There's a vendor you transact with, and your renewal's coming up. You owe them; it's a major software package—$100,000. You get that invoice with the payment details of how to send the payment, and you send $100,000.

Turns out what actually happened is that that vendor's email was compromised in some way, and the fraudster quietly monitored email communications and looked for an opportunity. They've basically set up a scenario where they're trying to get you to pay funds into an account by sending a fake invoice that's modeled after communications they've seen within that invoice.

They're seeing you message back and forth to that person. Or they'll even send messages and then delete them from that person's inbox right away and try to capture the responses before they can get them. They'll copy the invoices and give you bad wire details to send all those funds to. And with a wire, those funds are gone.

Businesses lose hundreds of thousands to millions of dollars when this happens because there's no way to get those funds back. There are ways to prevent it, and a lot of it is just extra due diligence. If this is the first time you've ever made a payment to this vendor, getting a verbal confirmation of those account details helps. It's like your own 2FA—an additional check that this person is who they say, and these are the right payment details. If this is a recurring payment and they suddenly email you that they have a new account, that's actually not that normal of a thing.

Businesses don't change their account details that often. That should trigger you to validate the transaction, just call them up and say, "Hey, I just want to double-check this invoice real quick. Is the amount right, the payment details?" Just to have the little additional check that that person actually did send that invoice. That is a new thing to be worried about. But that is definitely something that businesses, given that they do high-value wires, have to be concerned about. Usually, individuals who run into this are on the high net worth side doing business transactions anyway.

Q: Are there any misconceptions about ATO you'd like to dispel?

I'd reaffirm that business email compromise case. Thinking about ATO less from, "My account's been taken over." And thinking about it more from, "Do I trust the entry points of how I interact with my account?" Understanding that you could do everything perfectly and still be a victim of someone else's ATO scenario. If something seems off, there's a very real chance it could be off.

Ensure that you have good hygiene, not only on your own account but also in how you interact with other people. **Verbal communications are a good real-time 2FA for those types of situations where there's not really a better way to validate that information.**

Q: Is there anything you'd like to add that we didn't get a chance to cover yet?

Account takeover is not all doom and gloom. When I first started in Fintech, 2FA was not standard. Account takeover was way worse, and compromised passwords were a way bigger issue. Brute force attacks were a way bigger issue too. The industry as a whole has improved drastically, which is great because aaccounts are generally more secure.

Companies that prioritize account security will be better equipped to deal with the upcoming fraud schemes compared to other institutions. Companies like Mercury that invest in this ideally have this higher level of security that other institutions will be catching up to for a while as fraudsters adapt and mature. So, while the industry has improved, it's a shifting landscape. We always have to figure out what the next thing is and build a product around that.

Q&A With Tanya Corder

Q: Why is ATO such a popular form of fraud?

ATO (Account Takeover) provides fraudsters with direct access to victims' personal and financial information, which they can then use to commit other activities. If they have unauthorized information, they can make unauthorized purchases and open up new lines of credit, stealing victims' identities. Also, it's popular because of the ease of access to information. With the increasing use of online accounts and the internet, information is at the tips of their fingers, basically.

Also, for fraudsters, it's a large payout right away. Once fraudsters gain access to victims' accounts, they can potentially access large sums, also called hit and runs, where they take as much money as possible and disappear. It's a large payout, which is very attractive to them.

It's also difficult to detect when ATO happens. Fraudsters have seemingly mastered the ability to exploit their respective victim's accounts in ways that appear normal and therefore are able to succeed in continuing the nefarious activity for prolonged periods of time. It makes it difficult for victims to notice that their account has been compromised because the activity looks so normal. Whether it's small purchases that the fraudsters are making that look like normal purchases, as a victim, you might think, "Oh, I must have made that $10.99 purchase or whatever." There are definitely steps that can be taken, but whenever there is financial information available out there, fraudsters will find a way to abuse the system or gain access.

Q: Who's most at risk for account takeover?

Anyone (and everyone) is at risk for account takeover. Specifically, anyone who uses an online account or engages in eCommerce in any capacity is vulnerable. There are groups who are at higher risk for account takeovers. Elderly individuals who are less familiar with technology are susceptible to phishing scams or social engineering attacks. They are more likely to use weak passwords or reuse the same passwords across multiple accounts, making it easier for fraudsters to access them.

High-profile individuals who are well-known celebrities or public figures are also at higher risk for takeovers because their personal information is more widely available, so their accounts are more attractive targets for fraudsters. Finally, small business owners are also at higher risk than average. They generally have fewer resources to invest in cybersecurity or are more likely to use their personal accounts for business purposes, making it easier for fraudsters to gain access to both personal and business accounts.

Q: How do they get the information in the first place?

There are multiple ways. Phishing is one of them in which scammers send fake emails or text messages that appear to be legitimate to individuals or companies, to employees of companies, asking to provide account information. Where you click on a link, and it looks like a real one, and you enter information. Social engineering is another one where scammers use tactics such as pretending to be a customer service representative or IT support or something tricking the individual into revealing account information.

Leveraging malware, scammers record account login credentials or capture screen images of account information. Another big driver for account takeovers is through data breaches, where scammers obtain account information from a company or financial institution that has experienced a data breach.

Fraudsters have also become experts at leveraging public records. A lot of time, individuals display sensitive information such as addresses and phone numbers in a very public forum. For example, social media accounts also have a lot of public information where scammers obtain that information that can then be used to guess login credentials, answer security questions, or otherwise gain access by verifying credentials.

Fake applications and websites where scammers create phony applications that appear legitimate and are designed to capture account information when individuals enter their login credentials are another example.

Much of this seems to be depending on people being able to be super sleuths in terms of figuring out what's legit and what's not. Generations that didn't grow up with the internet from a very early age need to be really cautious.

Q: Are there distinct, predictable stages of what account takeover looks like?

The gathering of information stage is usually the first one. They'll gather information about their target email addresses, phone numbers, and social media profiles. That's done through various methods like social engineering or data breaches. Then there's phishing and malware delivery.

Once they have an email address, for example, they'll email the target an email that says "click on this" or send a phishing message designed to trick the individual into revealing login credentials. Then the next stage is the access, the account access, where they obtain the target's login credentials and they log into an account. Usually, they'll change login details or add their own contact information. For example, my husband and I have a joint banking account. They'll add another person, or another email, or something to the account.

Then after they gain access, that's where the fraudulent activity starts happening. They'll carry out unauthorized purchases or transfers of funds to other accounts, or sometimes once they access, they keep an eye out, and they don't necessarily make any activity for a while, but then they'll hit all of a sudden. Then, usually, there's something where they'll want to cover their tracks. Whether they delete browsing histories, disable security features, or something like that.

Q: Are there red flags that people can look out for?

Unexpected password resets, reset notifications, suspicious login activity on your account, unfamiliar devices: those are red flags to look out for. Unusual account activity. You might have a customer who is in the Pacific Northwest, and then all of a sudden, in the last three weeks, they've been logging in from the east coast or something. That's one thing to look out for. Again, changes to account information. All of a sudden, this person has a lot of different addresses or phone numbers that are added.

An increase in customer complaints is also something to look out for. **If there's an increase in customer complaints about unauthorized access or fraudulent activity, it might be a sign that an account takeover is occurring on the platform**.

If there are multiple instances on the platform, it may be a sign that there's a vulnerability in the system that is being exploited by fraudsters.

Q: And what red flags should organizations look for? Business email compromise?

Business email compromise is definitely something to look out for. I think attacks are specifically targeted on platforms through employees. For example, in businesses and organizations where fraudsters will impersonate a senior executive or trusted individual in the organization, they'll request an employee to transfer funds, provide sensitive information, or go to this website and log in and do this. Because it's coming from an exec, you're more likely to do it.

Fraudsters usually will do research on the organization and usually will do a little more planning with these account takeovers to identify personnel in the company that have access or are normally asked to do something like that.

Q: Aside from the obvious things like don't reuse passwords, use 2FA and and password managers, these kinds of things, what can organizations and individuals do to keep account takeovers from being a problem?

Software. **Keeping software up to date and security systems regularly updated can help prevent vulnerabilities that could be exploited by attackers.** The use of anti-malware and anti-virus software programs can help detect malware. Individuals should take advantage of those software that are available. Monitoring account activity closely is definitely something that both individuals and businesses can do. Regularly checking account activity for unusual activity can help identify account takeovers early and stop them before too much damage is done.

Regarding the use of email authentication protocols, there are ones that can help prevent email spoofing and phishing attacks. Then organizations can also conduct employee training and education. Training is a huge one. If employees know what to look out for, it definitely can prevent account takeovers from happening. The use of machine learning and artificial intelligence is also a huge one. It can be used to analyze accounts and activity and identify patterns that may indicate fraudulent activity or behavior. Then there's implementing multi-layer security measures such as firewalls, intrusion detection systems, security cameras, and things like that which can make it more difficult for attackers to gain unauthorized access to accounts with more sensitive information.

Q: Can you describe the one door, one key approach?

The one door, one key refers to a security principle that's used in physical security to access one room. The idea is that a single key, access card, or something is used to unlock only one door, and that key can't be used to unlock any other doors. That's to prevent unauthorized access to whatever room. Say the vault with all the cash or something.

To use this approach with an online account, you're using one password for this account. You're not using the same password over again. You have separate passwords for each account. That's what the one door, one key approach is.

Q: Are there any misconceptions or myths about ATO that you'd like to take the chance to dispel?

A lot of the red flags or even preventative measures that I've already mentioned. People who are at risk have repeating passwords. The myth is only individuals with weak passwords are at risk for account takeover. That's not true. Weak passwords certainly make it easier for attackers to gain access. Individuals with strong passwords, those generated-numbers ones, can still be accessed in various ways through phishing, social engineering scams, malware, and stuff. The myth is that weak passwords are the only ones that are at risk. That's not true. Really anyone is at risk.

Another myth is that account takeovers only affect individuals or small businesses and not large organizations. That's also not true. There are certainly lots of data breaches and data leaks from bigger companies, as well.

Two-factor authentication, there's a big myth that that's foolproof and prevents all account takeover attempts, and that's definitely not true. Attackers usually use some social engineering techniques to trick users into providing their two-factor authentication credentials or to bypass it altogether and stuff.

Let's see. Another myth is that once an account takeover happens, nothing can be done. There are definitely steps that can be taken to prevent further unauthorized access and recover any stolen funds. It might be a little hard, but there are still definitely steps that you can take to gain your stolen funds back. To prevent it from happening further on, you might reset your password, lock your accounts, or contact your financial institutions or law enforcement agencies. Get them involved and stuff.

Q: Any parting thoughts you'd like to include?

Prevention is key. Look out for the red flags, and change your passwords if you have this suspicious inkling. Be informed on the different techniques that scammers can use. Do your own homework periodically, as well. Make sure your software is up-to-date, and then report incidences and keep a record of your accounts.

21. "Q3 2022 Digital Trust & Safety Index: Account Takeover Data, Trends, and Insights." Sift Resources, Sift, 22 Mar. 2023, https://resources.sift.com/ebook/q3-2022-digital-trust-safety-index-account-takeover-data-trends-and-insights/.


fraud
detection
101

“The most sophisticated fraudsters are very professional. They’re running a business, and it’s their job to find who the most vulnerable company is.”

— Zach Pierce, Lithic

You know your fraudsters—the thieves, the con artists, the opportunists. You know how these bad actors steal and fabricate identities to take over accounts and unleash chaos. The question is how you can protect your organization and your customers from falling victim to fraud.

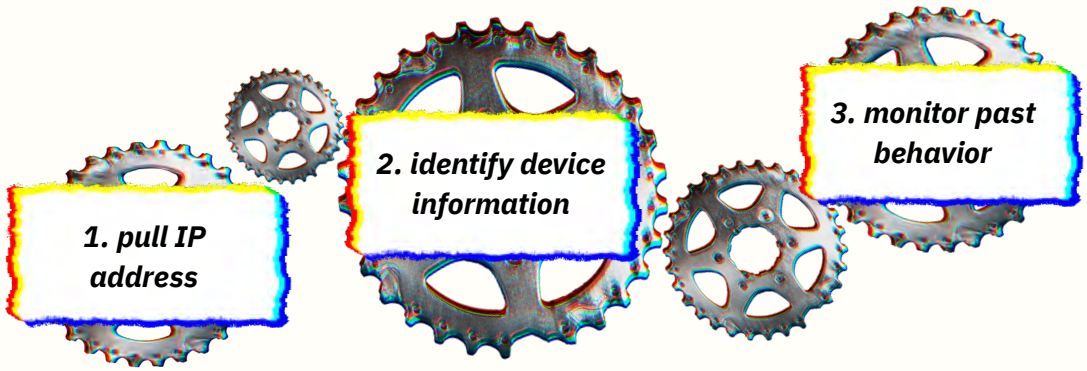
The answer is building a robust fraud detection system to help you remain one step ahead of bad actors and protect your business from reputational and financial harm.

To discuss this topic, we interviewed Zach Pierce, the Risk Operations Lead at Lithic, where he focuses on mitigating financial loss and building out the Risk team. Lithic is a card-issuing platform that caters to Fintech companies. He was the first risk hire, has been there about a year and a half, and leads a risk team that is at least in part focused on fraud detection. Before this, he was at Stripe, a payment processing platform that caters to all types of companies across the world. He worked on the risk team and was responsible for fraud detection, among other things.

For this chapter, he shared his knowledge, experiences, and opinions on the different types of fraud detection solutions, transaction monitoring, risk management, and the future of fraud prevention.

Types of Fraud Detection and Prevention Solutions

Organizations automate fraud detection with the help of rules engines, machine learning (ML) models, data enrichment tools, and hybrid solutions. Here's how these solutions work:



1. Rules Engine

As Zach explains, "A rules engine is an application that allows fraud detection agents to define rules related to a number of data points including user activity, metadata, and self-reported user information."

A rules engine generally works in three steps:

1. ***The engine is triggered as a result of a user action, like proceeding to checkout from their cart***
2. ***The engine uses the pre-set conditions and rules to decide which action to perform***
3. ***The engine performs the action based on the rules***

There can be simple rules, such as 'every transaction over $7,000 should be manually approved,' or complex rules that take the user's IP address, past behavior, device information, and other factors into consideration. With complex rules, you can also describe a variety of outcomes, such as sending the user an OTP or a verification link, reviewing the transaction manually, or rejecting it automatically. The most prominent advantages of using a rules engine are:

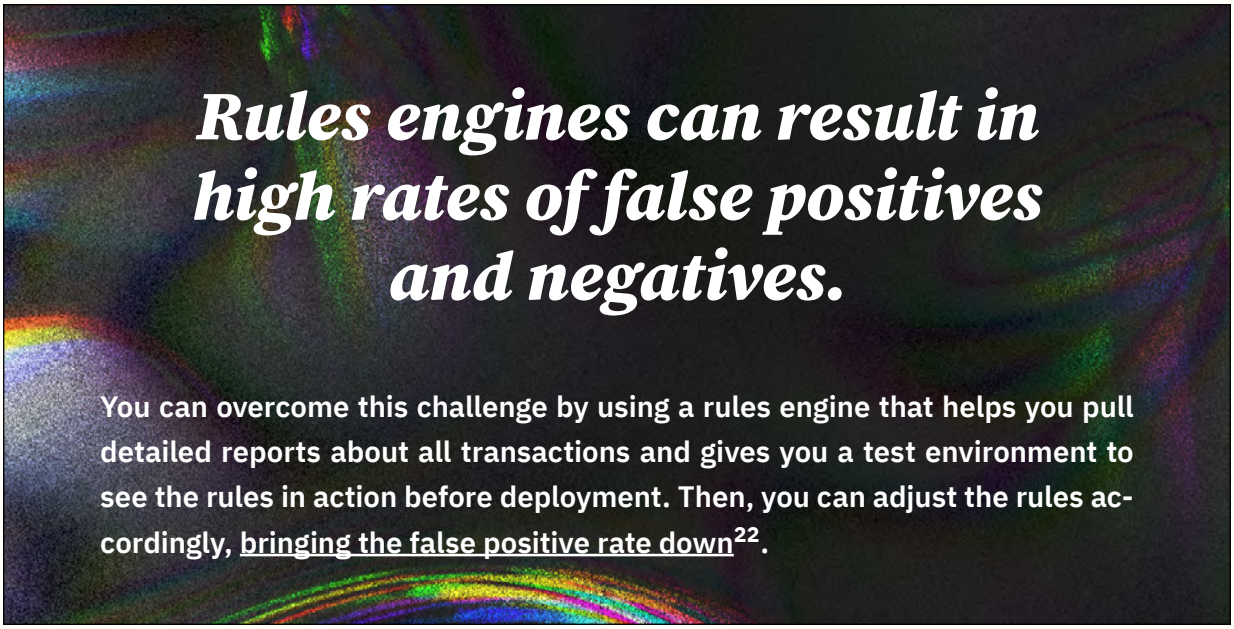
1. ***The rules are easy to deploy***
2. ***They allow you to monitor high volumes of transactions***
3. ***They help you respond to threats in a timely manner***

4. ***They result in valuable data, such as false positives and false negatives, which you can then analyze to create a more efficient and complex rules engine. A 'false positive' is a legitimate transaction that is declined due to overly sensitive rules. A 'false negative' is a fraudulent transaction that gets approved due to overly lenient rules***

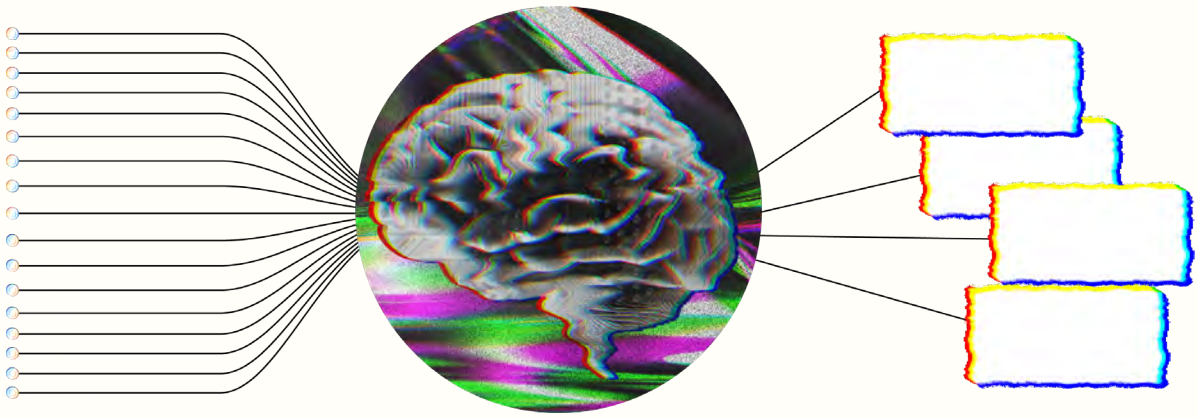
5. ***When implemented correctly, they can provide the perfect jumping-off point for the use of machine learning***

However, there are also some challenges associated with rules engines. If you choose to build your own engine, you will need a team of developers dedicatedly working for months—and there's no guarantee that you will build the kind of engine you want on your first attempt.

Building your own rules engine can prove to be a constant resource drain, rendering you incapable of scaling quickly. This challenge can be remediated by using a customizable solution that allows teams to set up and test rules without having to build the entire infrastructure from the ground up.



2. Machine Learning



Machine learning (ML) models are trained with the help of data generated by the rules engine, or a similar example dataset, to detect fraudulent behavior and outsmart fraudsters. ML systems are designed to handle large volumes of data, evolve as they handle more of it, and act instantly when they detect anomalies.

ML can be used to detect the same scams as rules engines. Some of the most common scams include phishing, forgery, identity theft, and credit card fraud. Some of these use cases need the algorithm to go through supervised learning, while others require unsupervised learning.

In ***supervised learning***, the algorithm needs labeled data and uses classification techniques[23] to determine outcomes (such as whether a link in an email is malicious or not). In classification, the algorithm 'classifies' data into different categories based on what it has learned from pre-categorized training datasets.

In ***unsupervised learning***, the algorithm uses unlabeled data and clustering[24] to find patterns and anomalies in data. Clustering means grouping similar data together without the use of any pre-categorized training datasets. These ML models are generally used to detect identity theft.

Zach notes, "Machine learning models can handle large volumes of data and identify new threats. But a drawback is that they are more time intensive and complex to set up and maintain than simple rules. It all comes down to how you have trained the algorithm and how you continue to optimize it."

It's important to note that ML models require large datasets to achieve higher accuracy, which not every organization has access to. The lack of human intervention also means less control and occasional false positives that could have been avoided with human input. For example, an ML model may flag a transaction coming from an unusual location without considering the fact that the cardholder may have traveled there.

There are two types of ML models when it comes to human intervention:

Black box machine learning: These are ML models that take action without giving any explanations behind their decision-making process. These models will flag a transaction without explaining why, and you won't be able to look into the logic behind the decision.

White box machine learning: These ML models have a transparent decision-making process. You can easily see the variables that affect each decision. Having that knowledge can help you train the model to make better decisions.

Many Fintech companies that use ML models often base all of their fraud prevention tactics around ML-generated fraud scores. Fraud scores are generated by ML models trained on transactions that have been marked as fraud by your company and/or other companies. Fintech companies often treat fraud scores as a silver bullet to solve all their fraud detection problems, but in doing so, they miss out on their own data and learning.

ML models trained on transactions that have been marked as fraud will eventually gravitate toward specific fraud patterns. To avoid that, you want to teach the model what genuine (good) activity looks like and what a "non-fraudulent" user looks like. One way to overcome that problem is to use 'alert scoring[25].'

What are alert scores?

Alert scores are scores assigned to fraudulent transactions on a scale of 0-100. They are generated by ML models that passively study the behavior of your rules engine. Alert scores are generated as a result of white box machine learning—and your team can easily understand why a particular transaction was assigned a higher score. Using this method helps you address the lack of human intervention that comes with black box machine learning.

3. Data Enrichment Tools

Data enrichment tools help you build a complete profile based on a few data points provided by the user. These tools augment data points such as email addresses, IP addresses, bank identification numbers (BINs), and device data. So, with access to a user's email address, data enrichment tools can find out if the email address is disposable or involved in past breaches.

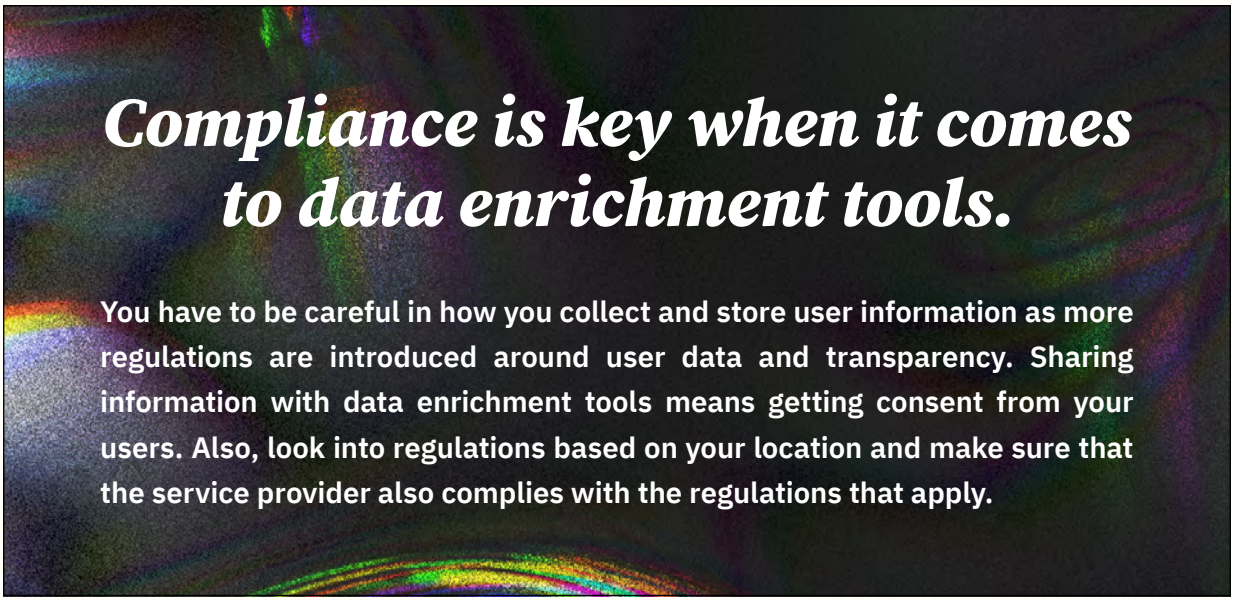
Zach has worked with both "enriched data and data that left a lot to be desired." The verdict? "Let's just say it made my life a lot easier when we had lots of accurate data to work with."

Data enrichment tools are usually integrated with the fraud detection system through point-to-point or third-party integration. User information is shared between the two systems to build a more detailed user profile through open source intelligence (OSINT)[26], the practice of collecting publicly available information from the internet.

These tools give you richer, more complete user profiles that improve the accuracy of your rules engines and ML models—and, consequently, improve your fraud detection rates. Data enrichment tools also help you maintain a frictionless user experience because the more you rely on them, the less information you have to collect from your customers.

"Working with data enrichment tools can be really helpful as they can give you information about a user that you wouldn't have access to otherwise. For example, if a user provides their phone number, you are not necessarily going to know who the carrier is, but that is something that you can get by using data enrichment from a 3rd party provider," Zach explains.

But while rich data is a tempting concept, enrichment tools aren't without risk. "Integrating with a new tool and building a process where information is shared between the two systems requires time, investment, and trust."



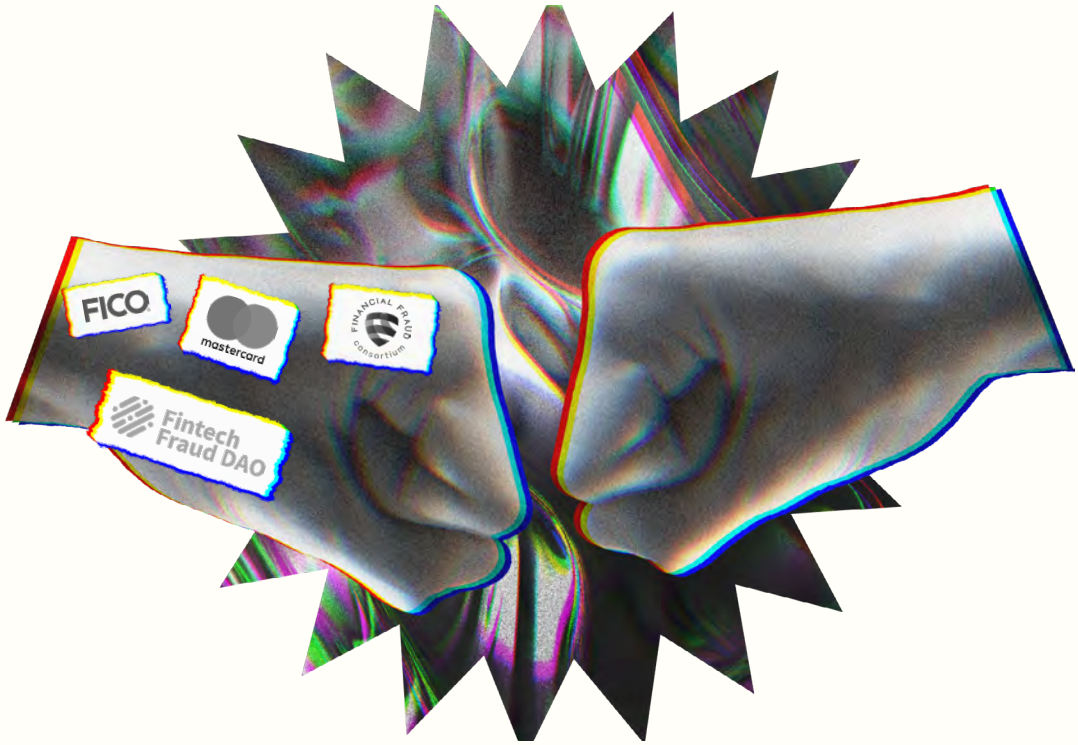
4. Consortium Data

A fraud prevention consortium is an association of businesses working together for a common cause. FICO® Falcon® Intelligence Network[27], Financial Fraud Consortium[28], Fintech Fraud DAO[29], and similar data consortia maintain large repositories of fraudulent payment data. These repositories are created through data sharing between multiple organizations.

In FICO's Falcon Intelligence Network, there are over 9,000 financial organizations[30] that submitanonymized data about legal and fraudulent transactions, trends, andtechniques. Joining the consortium and gaining access to consortium data can increase the efficiency of your rules engine as well as your ML model. You can simply take the consortium's decline list and tell your rules engine to decline all transactions coming from specific email addresses or credit cards.

Although consortium data provides useful information to feed your rules engine and ML models, Zach is skeptical. "I feel like not everyone would want to share information about fraudulent activity in their organization, especially since your competitors are also part of the consortium," he explains. This concern—that your competitors can access the data you share with the consortium—can be alleviated by aggregating, anonymizing, and encrypting all data shared by members of the consortium. Fintech Fraud DAO uses these techniques. It is a decentralized network of Fintechs, so no single entity owns all the data shared by the members.

Keep in mind that decline lists and lists of terminated merchants might contain outdated data—the bad actor could have already used a credit card and moved on to the next by the time you block the card that's no longer in use. Consortium data also punishes people who are victims of identity theft, a compromised email address, or a stolen credit card since they might find themselves blocked by thousands of organizations with access to this information.



Decentralization is the way forward for all consortia.

If all members of the consortium collectively make decisions about the policies that govern consortium data and data storage is decentralized, more and more organizations can be encouraged to join consortia and share their data and experiences related to fraud detection.

Transaction Monitoring Best Practices

Bad actors commit fraud to steal money, goods, and services—and the act itself happens in the form of transactions. Transaction monitoring is one of your best bets to stop fraudsters cold in their tracks.

1. Use a Customizable Platform for Fraud Risk Management

There are many transaction monitoring vendors and pre-built solutions out there. Use those that can be customized to meet your specific requirements without the help of engineering support. Otherwise, you run the risk of the vendor solutions being too rigid to adapt to your unique challenges.

"If you're like Lithic, an infrastructure company that caters to Fintech companies, this whole assumption of how we work and how transaction monitoring works for us doesn't hold true for most off-the-shelf transaction monitoring tools," explains Zach. "So, in that case, it makes more sense to go with something more flexible."

Customizable rules engines give you that flexibility. They come equipped with pre-built rules based on recommendations by financial fraud analysts. But you can change those rules, set your own rules, test them, transform the engine into a tool specific to your use case, and achieve high rates of accuracy.

Even if you achieve the highest rates of accuracy with your current rules, bad actors will continue their attempts to defraud you. So, keep optimizing your rules and keep an eye on false positives and negatives.

2. Be Proactive in Your Approach to Fraud Detection

Most companies are reactive in their approach to fraud detection. They get defrauded in one particular way and take measures to protect themselves from it, only to get defrauded in a different way later on. You don't always have to learn things the hard way. Here's what you can do to be proactive in fraud detection and prevention:

- ***Use the expertise of fraud detection professionals, such as compliance officers, to understand the potential threats in your industry***
- ***Build a list of events that should be tracked by your system***
- ***Create rules and describe in detail the actions that should be taken when suspicious activities are detected***
- ***Implement a software that would track events and establish rules***
- ***Keep improving your list of events and rules to account for new threats***

3. Focus on Data Governance To Get Higher-quality Data

Data governance[31] is a collection of rules, policies, and processes that ensure the availability, integrity, and security of data in an organization. With the help of data governance, you will integrate data silos, deal with missing, incomplete, and erroneous data, and turn unstructured data into structured data. That means you will have higher-quality data to analyze and feed to your ML model, reducing false positives and negatives and ultimately improving detection rates.

Data silos are a big challenge, especially in large organizations. You can overcome this problem by using a transaction monitoring system that tracks all data points related to user activity and stores them in a way that they are accessible and available to you for analysis as needed.

4. Think Like a Fraudster

In the first chapter, we learned all about first-party, second-party, and third-party fraud. We also discussed multiple types of fraudsters from opportunists to identity thieves and criminal organizations. While there are many types of fraudsters, they all have one thing in common—they are always trying to figure out your vulnerabilities.

Just as fraudsters are constantly trying to figure out your rules engine, you have to study their tactics to see how they may attack you. For every community and consortium dedicated to fraud detection and prevention, there's a space for bad actors. Just as we write detailed guides on fraud detection, they write guides on how to commit fraud and how to get around rules engines. If you can gain access to that information, it will help you figure out how fraudsters think and stay one step ahead.

"One thing I like to do is figure out the most expensive part of their business model and make it more expensive," says Zach. "For example, I'd get them to burn more credit cards than usual before they realize that their transactions are unsuccessful."

The Dynamic Approach to Fraud Detection

When using a machine learning model, you can monitor each transaction using either a dynamic approach or a sequential approach. The dynamic approach monitors real-time data. In sequential modeling, the ML model analyzes a sequence of events and tries to detect anomalies.

In the dynamic approach to fraud detection, ML models monitor real-time data to identify fraudulent activity. The models are trained on historical data and use transaction data, user behavior data, and external data sources to detect new patterns and flag suspicious activity. It is a proactive approach to fraud detection, and it is responsive to new threats, providing businesses with the tools they need to stay ahead of fraudsters and protect their customers and bottom lines.

If a company chooses to use machine learning, it can combine both approaches. The sequential approach should be on auto-pilot, with each flagged sequence being sent to the team for review while they work with alerts being sent their way through the dynamic model. That will help improve the overall fraud detection system by combining sequences, real-time detection, and human intervention.

Risk Assessment Best Practices

Risk assessment is a critical component of fraud detection, as it helps businesses identify and prioritize the highest-risk transactions and entities. The essential components of risk assessment in fraud detection are:

- ***Data collection:*** Collect data from customer profiles, transactions, and external sources.

- ***Risk scoring:*** Assign a risk score to each data point based on the likelihood of fraudulent activity.

- ***Defining risk thresholds:*** Determine the minimum acceptable risk score of a transaction. Any transaction exceeding the risk threshold should be flagged.

- ***Establishing investigative procedures:*** Once a transaction is flagged as suspicious, it has to go through investigative procedures. Define these procedures and document them.

To improve fraud detection, the team working on risk assessment should focus on developing a solid understanding of the business. If third-party auditors have been brought in for risk assessment, they should work with heads of departments to get to know the products and services offered, the customers served, and the potential fraud risks associated with each transaction.

Zach provides an example of what this process entails: "For example, if you are a neobank, your points of risk are anywhere money is coming in … and where money is going out. So, learn about how the bank operates, how different types of transactions work, how loans or credit cards are approved, how applications are processed, and so on. That will help you understand how different areas can be abused by bad actors."

Risk assessment reports for different organizations will differ greatly based on their industry, processes, size, geographical location, customers, and more variables. However, all risk assessment reports should have the following information:

Risk profiles: Risk profiles are a detailed compilation of all risks faced by a company. These are built after an assessment of all company processes involving customers, employees, partners, and other stakeholders.

Risk categories: Risk categories consist of different risks grouped together based on their type. For example, risks such as distributed denial-of-service (DDoS) attacks and malware attacks can be categorized as cybersecurity risks.

Risk sources: As evident by the name, risk sources are all external and internal factors that may affect your overall risk. For example, each type of transaction that moves money in or out of your system is a risk source.

Overall, assessing risks to improve fraud detection requires a combination of technical expertise, data analysis skills, and an understanding of the business. "That combination of knowing your business, knowing where the money moves, and then the different sort of fraud archetypes helps you in risk assessment," says Zach.

The Future of Fraud Detection and Prevention

Fraud detection, and how organizations tackle it, has evolved over the last few years. “When I was at Stripe, and we were building machine learning models, we had a team full of people that had PhDs,” recalls Zach. “Now [the technology] has become much more accessible … with the help of out-of-the-box tools. Seven years ago, we had to build a fraud detection system from the ground up. Now there are out-of-the-box solutions out there that you can use.”

“Similarly, there are a lot of low-code solutions that help non-engineers,” he adds. “The way I see it, low-code tools will continue to empower fraud detection professionals in the future.”

Key Takeaways

Fraud detection is all about building a robust system that can quickly take you from being reactive to being proactive about fraudulent transactions. To do that, you can rely on:

Rules engines: They help you define and implement rules related to user activity. Advantages of rules engines include ease of deployment, the ability to monitor high volumes of transactions, and the collection of valuable data.

Machine learning: Trained on large datasets of fraudulent and legitimate user activity, ML models can evolve with new data and act without human interference, but they are not without challenges.

Transaction monitoring is a major component of any fraud detection system. To maximize its effectiveness, companies should:

Use a customizable platform: So you can make rules specific to your requirements.

Focus on data governance: So you can take control of your data and improve data quality and accuracy.

Think like a fraudster: So you can find potential vulnerabilities in your system.

Now that you have a baseline for what tools to use and how to use them effectively, the next step is to learn how to assemble the right team and create a culture where everyone’s on the same page about the importance of fraud detection and prevention.

Chapter 6 will focus on risk operations, including how to justify the investment into fraud prevention programs, what success metrics to measure, and how to build a collaborative risk culture within your organization.

Q&A With Zach Pierce

Q: What is a rules engine? What are some of the advantages of using a rules engine for fraud detection?

A rules engine is a software program that allows fraud detection agents to define rules related to user activity. They help you respond to threats instantly, build a database that you can use to constantly improve your fraud detection system, and go from a reactive to a proactive approach.

Q: How do you use machine learning for fraud detection? What are the advantages and disadvantages of using machine learning?

You build machine learning models with the help of training data. This is data that can help the algorithm understand the difference between legitimate and fraudulent transactions. As for advantages, machine learning models can handle large volumes of data and identify new threats. But a drawback is that they are more time intensive and complex to set up and maintain than simple rules. It all comes down to how you have trained the algorithm and how you continue to optimize it.

After deployment, ML models can react quickly to fraud patterns and offer a greater level of flexibility than rules since rules need to be explicitly defined.

Q: When it comes to fraud detection, do you think using a rules engine is a good idea, or do you think that machine learning is a better alternative?

I think it is best to take a hybrid approach. Rules engines are nice in a few different scenarios, and when you're first starting out, they're typically all you've got. And they can be what you use to build the data set that lets you then move on to building a machine learning model. They can also be useful as a backstop because if you train machine learning models on a bunch of different features, you know, they're going to look for what they're going to look for, but there's no guarantee that they will catch potential catastrophic loss. So, if you want to set some kind of rule that's like, 'any $10,000 payout gets looked at by a person,' you could do that through a rules engine.

Q: Do organizations necessarily have to use a rules engine first and then move on to machine learning?

I've heard there are vendors out there that have sort of out-of-the-box-type models that might help you if you're dealing with credit card transactions. They share their machine learning models, or rather, the findings of their machine learning models, so it's not necessarily true that you need rules to start.

But, using a rules engine helps you build a healthy database full of information about legitimate and fraudulent transactions. By using a rules engine in combination with machine learning, you can train your ML model off of your own data. Usually, a rules engine is the easiest thing to start with. Just set some very basic rules and then measure how well they're doing, and then start a feedback loop of making it better and better.

Q: What are data enrichment tools? What are the pros and cons of using data enrichment tools?

Working with data enrichment tools can be really helpful as they can give you information about a user that you wouldn't have access to otherwise. For example, if a user provides their phone number, you are not necessarily going to know who the carrier is, but that is something that you can get by using data enrichment from a 3rd party provider.

I think you can get a lot of value out of them. For example, locating IP addresses or finding out what banks associate with what routing numbers, cell phone carriers associate with phone numbers, if someone is using a Voice Over IP, or a cell phone, or a landline; those are very useful.

But **integrating with a new tool and building a process where information is shared between the two systems requires time, investment, and trust**.

I haven't personally worked directly with data enrichment tools, but I have had the experience of working within organizations where we had access to a lot of data as well as places where data was limited, and let's just say it made my life a lot easier when we had lots of accurate data to work with.

Q:What is consortium data? What are the pros and cons of using consortium data?

A consortium is a group of organizations that share data with each other for fraud prevention. I've honestly never really used this outside of the stuff that you kind of have to use when you're dealing with credit cards, like Mastercard's MATCH database. I see the value, in general, of having a list of merchants that have been terminated at your disposal to check against for making onboarding decisions. But I haven't personally gone out and used any sort of consortium data. I feel like not everyone would want to share information about fraudulent activity in their organization, especially since your competitors are also part of the consortium.

Q:How have different techniques of fraud detection and prevention evolved in the last few years? Have you seen any major progress in this field in general?

I don't think I have been around for that long to comment on this. But I think that the one change that I've seen is that technology is a lot more accessible now than it was seven years ago. When I was at Stripe, and we were building machine learning models, we had a team full of people that had PhDs, and now you don't need that anymore. Seven years ago, we had to build a fraud detection system from the ground up. Now there are out-of-the-box solutions out there that you can use.

Detention and prevention tools have become much more accessible.

Q:Which is the most commonly used technique to build a robust fraud detection system? Is it machine learning or rule-based fraud detection?

I can only really speak to the places I worked, and they definitely use both. I think rules engines are a great place to start and grow. When you see brand new activity and you need to respond to it immediately, a rules engine is more useful because it's much quicker to create a new rule than train and deploy a new ML model.

Q:How do you see fraudsters most frequently defeating fraud detection?

I think the most sophisticated fraudsters are very professional. They're running a business, and it's their job to find who the most vulnerable company is and who they could defraud. So, they're constantly finding new targets, testing new methods, and using new data that's become available—like new stolen identities and new dumped credentials.

So, I think it's that sort of relentlessness and continuing to test people that is how they ultimately get in. We're kind of in a unique position at Lithic because our customers are Fintech companies, and we see fraudulent actors hit one company, and then move to the next, and then go somewhere else. So, I think it's that persistence and the fact that they are professionals.

Sometimes it is amateurs in their bedroom trying to make fraudulent transactions, but a lot of the time, it's professional criminals, and they also have an understanding of how these systems work, how machine learning is trying to catch on to them, and so on. They write guides and share them on the dark web. You can read them, and a lot of times, they get stuff right. Sometimes they get stuff wrong; they think that you're doing things that you're not, which is actually kind of useful. Like if they think you're checking consumer credit scores or something, but you actually aren't, it's useful because it makes the identities they have to acquire more expensive.

Q:How does an organization move from fraud detection to fraud prevention?

Fraud detection is reactive, and it's typically where you start off because you're learning about your product and how it can be abused. I think **fraud prevention is when you shift to being more proactive, so you know what you're looking for, and you can look for the early indicators of it.**

Also, as I mentioned, fraudsters are running a business. One thing I like to do is figure out the most expensive part of their business model and then make it more expensive. It makes you much more unattractive to them. So, if the most expensive part is using stolen credit cards, for example, I'd think of ways to get them to burn more credit cards than usual before they realize that their transactions are unsuccessful.

Q: Do you think companies should build their own transaction monitoring tool or get it from a vendor?

I think it really depends on what kind of business you are in because, from what I've seen of the transaction monitoring vendors, a lot of them have a particular customer archetype in mind. If you have a straightforward use case where you are issuing single cards or accounts to consumers or SMBs, a vendor solution can work great because that is the customer they tend to have in mind.

But, if you are a Fintech company with a very complex use case, the vendor solutions can start to break down. For instance, if you're like Lithic, an infrastructure company that caters to Fintech companies, the assumptions that many vendors make around their data models and how their product works doesn't always translate because Lithic's customers are more complex than the ones the vendors build their products to serve.

Q: How do you adjust your strategy if false positive rates are high?

Typically, what you're trying to do with transaction monitoring is you have your human bandwidth to review transactions, and then you're trying to maximize the ROI of that human bandwidth. So, you're trying to have it focus on the higher-performing rules that catch the most interesting things.

If false positives are high, it could be because your rule criteria is too broad, or perhaps your rules are working fine, but the people making the decisions are not trained properly or don't have access to the right pieces of data that would enable them to make the correct decisions.

However, if your rules are too narrow, your system might not generate any alerts, which is also a problem.

It's really just a matter of having the right visibility into how everything is performing so that you can notice where things are going wrong. **You should be measuring all of these possible causes to the best of your ability so that when something like this comes up, it is easy to diagnose and make adjustments to counteract**.

Q: What are the essential components to risk assessment? On a practical level, what should companies do to assess their risk better?

I think the things that are the highest risk to me are any places where money moves. For example, if you are a neobank, your points of risk are anywhere money is coming in from bank accounts or other sources and then where money is going out in the form of payments or bank transfers. So, learn about how your business operates, how different types of transactions work, how loans or credit cards are approved, how applications are processed, and so on. That will help you understand how different areas can be abused by bad actors.

The less obvious things to think about though are the things that cause you to incur costs and if they can be abused. For example, many companies verify bank accounts using micro-deposits in cases where authentication through Plaid or someone similar isn't available. The company will send a small amount of money, usually less than $2, and ask the user to confirm the amount. But there are fraudsters out there who will exploit this and go through hundreds or thousands of micro-deposit authentication attempts in order to steal money from you. There are similar vectors to think about around network fees from declines and things of that nature.

I think it's helpful to have some knowledge about the kind of risks the business faces and vulnerabilities that could be abused. So, **that combination of knowing your business, knowing where the money moves, how costs are incurred, and then the different sort of fraud archetypes helps you in risk assessment.**

Q: How do you see fraud detection and fraud prevention moving forward? Will AI play a role in this area?

I don't really see too many immediate changes. In theory, you can use ChatGPT to generate a phishing email, but I don't think it's going to have any impact on how we detect fraud.

I do think, down the road, AI image generation will become pretty concerning, especially if you can generate very convincing images of people holding up their driver's licenses. Because one of the most challenging forms of authentication to beat is someone holding up their driver's license in a selfie, if AI can be used to fake that, especially to the point where it isn't easily detectable, we may need tools that haven't even been developed yet to counter that.

Q: What fraud detection technologies get you the most excited?

This isn't necessarily just restricted to fraud detection technologies, but there are a lot of low-code and no-code solutions that help non-engineers build internal tools and systems. These no-code and low-code tools have helped us move really fast in situations that'd otherwise need engineers. The way I see it, low-code tools will continue to empower fraud detection professionals in the future.

Q: Do you see any specific challenges regarding fraud detection and prevention that organizations struggle with today?

I think the proliferation of neobanks and crypto exchanges was pretty big over the last few years. Acquiring a bank account used to be pretty high friction, but with neobanks, it became a very low-friction process, which meant it was much easier to create a bunch of bad accounts.

Likewise, I think crypto exchanges became a very attractive target for bad actors to exfiltrate funds. But I think that both of those are kind of waning a little bit. So, right now, there's nothing brand new in terms of challenges that organizations struggle with today, but the things I mentioned are definitely very much in play.

21. "Bakkt: Case Study." Bakkt | Case Study, Unit21, https://www.unit21.ai/customer-detail/bakkt.

23. Banoula, Mayank. "What Is Classification in Machine Learning?: Simplilearn." Simplilearn.com, Simplilearn, 29 Mar. 2023, https://www.simplilearn.com/tutorials/machine-learning-tutorial/classification-in-machine-learning.

24. "Clustering Algorithms | Machine Learning | Google Developers." Google, Google, https://developers.google.com/machine-learning/clustering/clustering-algorithms.

25. "Alert Scoring: Prioritize the Alerts That Matter with unit21." Unit21 Blog, Unit21, https://www.unit21.ai/blog/alert-scoring-prioritize-the-alerts-that-matter-with-unit21.

26. Sharma, Ax. "What Is OSINT? 15 Top Open Source Intelligence Tools." CSO Online, CSO, 28 June 2021, https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html.

27. "FICO® Falcon® Intelligence Network." FICO, https://www.fico.com/en/fico-falcon-intelligence-network.

28. "Combating Risk & Fraud." Financial Fraud Consortium, https://fraudconsortium.org/.

29. "Fintech Fraud Dao." Fintech Fraud DAO, https://www.fraud-dao.com/.

30. "Falcon Intelligence Network: A Fraud Consortium for Fraud-Fighting Machine Learning Innovation." FICO Decisions Blog, https://www.fico.com/blogs/falcon-intelligence-network-fraud-consortium-fraud-fighting-machine-learning-innovation.

31. Stedman, Craig, and Jack Vaughan. "What Is Data Governance and Why Does It Matter?" Data Management, TechTarget, 31 May 2022, https://www.techtarget.com/searchdatamanagement/definition/data-governance.

RISK

RISK

RISK

OPERATIONS

OPERATIONS

OPERATIONS

OPERATIONS

OPERATIONS

OPERATIONS

“There will never be zero risk tolerance. We need to align on where we will fix and where we are willing to take a calculated risk. And that’s why it’s always a moving scale.”

— Rajeev Muppala, Brex

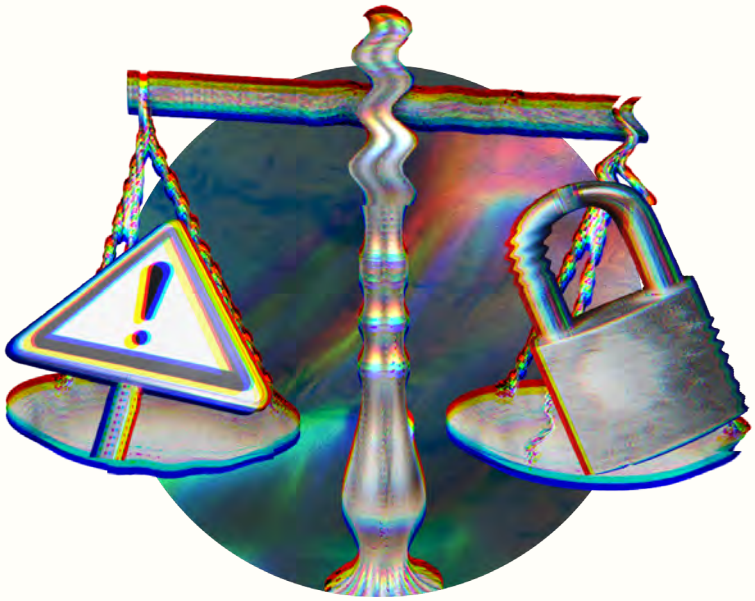
Whether it’s cryptocurrency fraud, synthetic identity fraud, account takeovers, or traditional transaction monitoring, your risk operations team holds the key to protecting your organization and your customers from external threats. But building an effective risk operations team requires investment, collaboration, and a shared understanding of the threats your company faces.

To get an inside view of risk operations, we interviewed two experts from Brex, a company that provides cards and money management products to startups and enterprises. Rajeev Muppala is the Head of Risk Ops, with oversight over three key areas: Know Your Customer (KYC), Fraud Risk & Operations, and Enterprise Risk Analytics. This involves implementing strategies and protocols to ensure compliance with regulatory requirements, mitigating fraud risks, and developing tools and frameworks to analyze and manage enterprise risks. Ali Rathod-Papier is the Head of Financial Crime while also serving as the BSA (Bank Secrecy Act) officer.

In this chapter, we cover tips for assembling a risk operations team, how to justify investment into fraud detection and prevention, ways to communicate effectively with other departments and create a culture where risk mitigation is understood, and what to measure to assess the performance of the fraud program over time.

Justifying the Investment

Smaller organizations are often more reluctant than larger ones to invest in robust risk management because the resources must be managed more carefully in a small organization. Small businesses are particularly vulnerable due to their limited resources and often lack the necessary controls to prevent and detect fraud. But regardless of size, it's not uncommon to find resistance when it's time to invest in fraud risk management. Here are tips for convincing leadership that investing in fraud risk management is worth the time and resources.



Link Fraud Risk Management to Business Goals

Senior leaders are used to thinking about the organization in business terms, so try speaking their language. If you can help them see how investing in risk management can help them reach their goals, you're more likely to get buy-in.

Ali recommends explaining to leaders exactly how risk operations will help them reach their business objectives. Connect the dots for them.

Rajeev uses an example: In Fintech, it's common to partner with a traditional bank. "This does not obliterate the Fintech's responsibility from the need to adhere to certain regulations and compliance requirements."

But traditional banks are traditionally strict about fraud prevention measures. Ali lays out the argument: "This banking partner is asking these questions, and if we don't respond, and we don't have a good answer, they're not going to work with us. And so, if the business can understand it as 'these compliance things will be blockers if you don't do them,' that tends to be quite effective."

Point to Similar Companies in Your Space

Using real-life examples can offer an added impact. “I think having that real-life situation can help incentivize people,” Ali says. Companies of a similar size in the same industry make the best examples.

If you were trying to underline the importance of preventing a data breach to an enterprise in Fintech, you might remind the leadership team of another Fintech organization that faced significant financial losses and permanent damage to its reputation after a data breach let fraudsters get access to customer data.

This tactic can be especially effective when you need to emphasize the potential hazards of less immediate risks. “You have less convincing to do when it comes to fraud risk because if the company loses money, it will fix it,” Rajeev says. But compliance risks can take years to become a problem, so it can be tempting to ignore. That’s why it’s important to show the leadership team the stakes of being out of compliance with laws or regulations.

Rajeev points out that the compliance risks can be severe: “This is where companies and management or boards that have discounted risk management have had to face heavy burdens, terminations, and sometimes complete dissolution of the company itself.”

Prioritize Your List of Needs

If you anticipate resistance, break down your list, so you can get buy-in for the things that are most important and present an immediate risk to the organization. Start with the investments that are absolutely required, whether that’s because of regulations or the goals of the company.

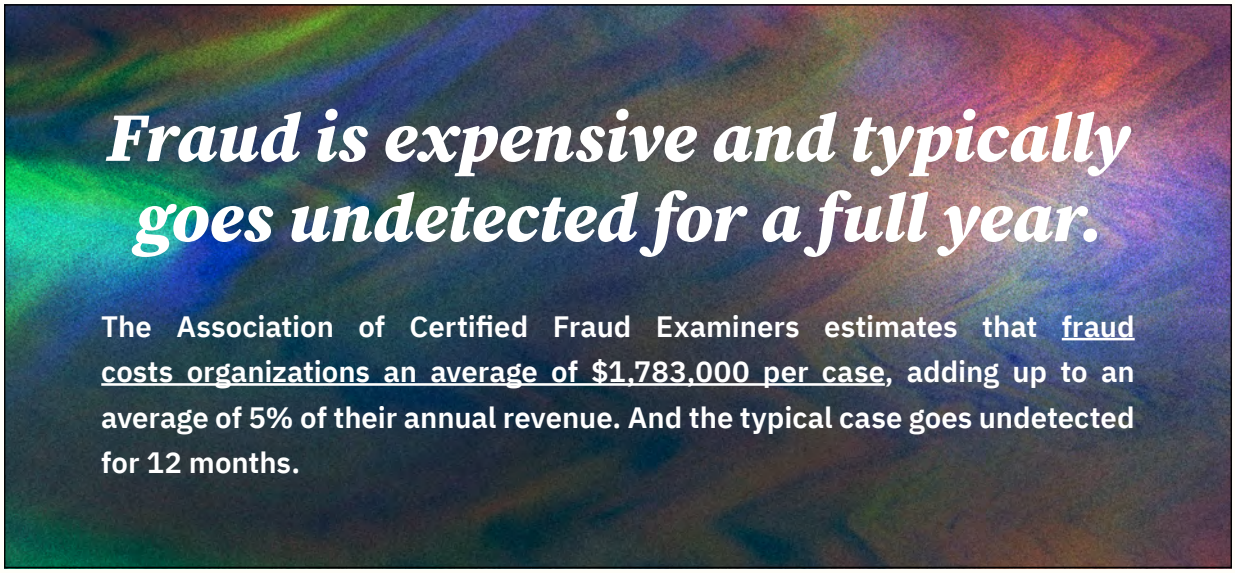
Better to start small and build up to a robust risk management system than to have nothing at all. If the company deals with sensitive customer data, investing in robust security and privacy measures would be absolutely required. Another example could be investing in updating outdated software or hardware that poses a security risk.

Then list everything that would be nice to have, along with a description of how the investment would pay off. You can slowly start to prove ROI, which will then convince leadership to continue to invest in the nice-to-haves. Finally, create a list of investments that don’t need to be done now but will be important in the future.

Create a Clear Impact Assessment

To make the ramifications of each investment choice clear, outline both the immediate and the long-term impacts of each investment.

“Compliance risk is always two, three years down the line,” Rajeev points out. And in a Fintech, it is typical for the leadership to think of immediate financial risk. It helps to talk about the risk of financial losses they’re taking if they don’t invest in risk mitigation.



Building the Team

To build your team effectively, you first need to know what key functions are most important for your organization’s needs. Rajeev recommends four roles or mini-teams (depending on the size of your organization):

1. ***KYC, AML, and EDD (enhanced due diligence)***
2. ***Transaction monitoring and customer sanction screening***
3. ***Fraud strategy and governance***
4. ***Fraud prevention and detection***

Finding the right people is critical for building an effective risk operations department.

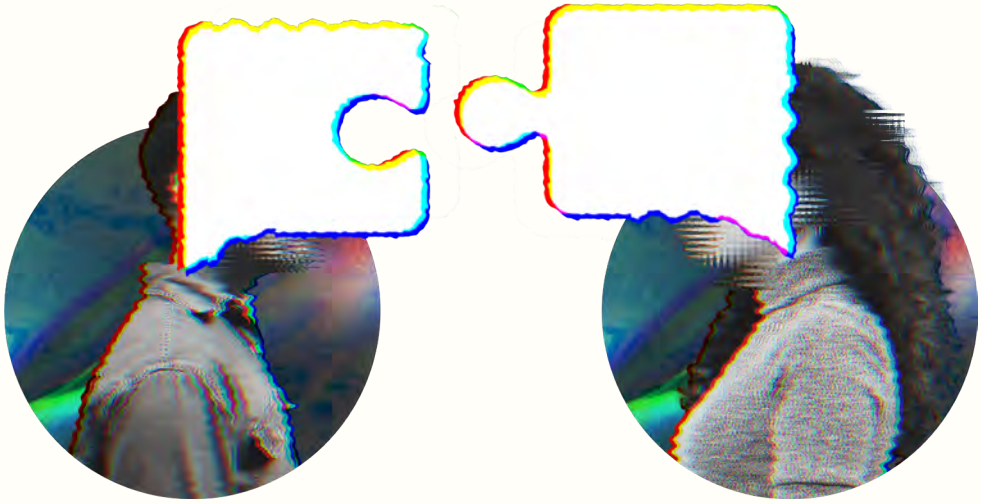
Who joins the team is top of mind for leaders in risk operations. In a 2022 PwC survey of risk management executives, 75% said that hiring and retaining talent is very important to their company growth.

Overall, your team needs to be able to factor in the greater context in any given situation to determine whether or not the activity is unusual. “Because if you don’t have the context,” Rajeev says, “you will not be able to make an informed and effective decision.”

To be capable of the kind of contextual judgment required for fraud risk management, team members must know the industry and have a solid understanding of the product the company creates. Rajeev emphasizes that they should also possess curiosity, problem-solving skills, and attention to detail.

How To Promote Cross-Departmental Collaboration

Cross-departmental collaboration is essential for successful risk management, but it can be challenging to achieve due to differences in department priorities, resource constraints, and communication styles.



Communicate Constantly and Share OKRs Across Teams

Sharing OKRs across teams can keep everyone working toward the same goals, which boosts collaboration and alignment between departments. But to do that, all your teams will need to communicate and be humble enough to ask each other for advice.

“Our priorities could be different when it comes to the day-to-day,” Rajeev says, “but there also needs to be some aligned priorities.” So, check in frequently with other teams and make sure you’re aligned.

Rajeev uses his own team as an example: “We have a separate risk and access team within the product team, where they collaborate with [Ali and me] day in and day out,” he says.

“What should we look out for proactively? Ali, can you tell us if we need to look at this regulation or that regulation? From a fraud standpoint, what kind of fraud pressures will we see if we introduce this in this market? And the reason why we have been moderately successful is we both share the same OKRs. We have to answer to the same leaders.”

This can be especially important for risk operations, which require cross-departmental collaboration to be successful. Customer service, marketing, and sales need to be aligned to prevent fraud because if there are gaps between these departments, it can create opportunities for fraudulent activity. For example, if customers receive conflicting information from sales and customer service, they may be more likely to fall for a scam or phishing attempt. If they see that the company is not aligned, the red flags of a phishing scam may just look like a disorganized company. By aligning these departments, a company can create a unified front to better prevent fraud and protect its customers.

By sharing some OKRs with other teams, employees get more insights into each other's priorities and work together more effectively to prevent and detect fraud.

Set the Tone From the Top

When leaders of different departments including product, engineering, customer service, and sales, for instance, share the same vision and goals, the rest of the teams are more likely to be aligned and understand how their individual work contributes to the company's overall objectives.

This can lead to better communication and cooperation between departments, reducing the risk of fraudulent activity and, ultimately, benefiting the customer experience. This alignment is crucial because it ensures that everyone is on the same page and working toward the same objectives. It also helps prevent confusion and miscommunication, which can lead to inefficiencies and mistakes.

For example, the customer service department might promise a customer that a certain security feature is coming out on a certain date, but the engineering team has actually run into a delay. If the engineering team hasn't shared the new release date, the customer service team might be making promises they can't keep. This could potentially lead to negative reviews or customer churn. By aligning these departments and ensuring that they are aware of each other's actions, the company can prevent these types of mistakes and provide a better experience for its customers.

Successful risk management requires ongoing evaluation and strategy revisions to adapt to new threats as well as organizational changes—inefficiencies and mistakes slow down this ability for adaptation.

Build Cross-departmetal Relationships

Building relationships between individuals across departments is especially important in a Fintech environment where fraud prevention is a top priority. By working together, teams can identify and address potential vulnerabilities in the system and implement controls to prevent and detect fraud.

Work To Establish a Compatible Communication Style

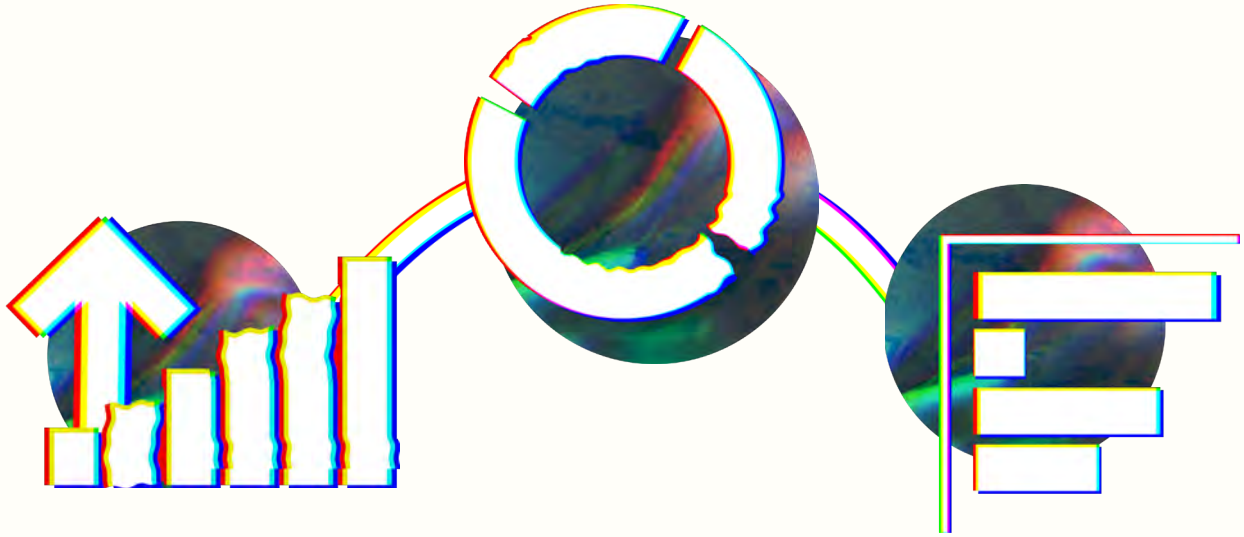
Different teams work differently, and that often extends to the way teams communicate. Making an effort to find common ground in the way you communicate with other teams allows teams to work together effectively and avoid misunderstandings or conflicts. Teams may have different communication styles based on their work culture, priorities, or industry standards. Failing to find common ground can hinder collaboration and slow down progress.

Say you need to collaborate with the customer support team to investigate potential fraud cases. The customer support team might communicate more casually and collaboratively, while the risk operations team has learned to be detail-oriented and exact in every communication to ensure regulations are followed and nothing is missed. A compromise here might include adding warmth and pleasantries into communications when interacting with the customer service team while explaining why and when certain communications need to be specific and direct.

Performance Metrics

The job of building a risk operations team is never really done. As a team, you must continue to revise the strategy to prevent threats.

“Businesses are never static,” Ali points out. “Whether you are a small, fast-growing Fintech or you’re a huge global financial institution, your products and services are going to change.”



To keep up with fraudsters, risk operations teams need to keep learning.

In a 2022 survey, the top challenge respondents expected over the next year was “availability of skills” at 20%. Rated just below were “data governance” and “cyber resilience” (both 17%).

To evaluate how well the team is doing in mitigating risk at your organization, ask them key questions:

What risks exist in the team or with the product? And what is the likelihood that these risks will actually happen?

Why it's important: Identifying risks allows the team to proactively mitigate them and prevent potential issues.

Metrics to include: Risk assessment reports, frequency and severity of incidents related to identified risks, and success rate of risk mitigation strategies.

Example: A risk identified in the product is the potential for data breaches. The likelihood of this risk can be measured by analyzing past incidents, identifying vulnerabilities in the system, and assessing the current security measures in place.

How effectively are we mitigating these risks? What controls are currently in place? What kind of alert exists, and how often is reporting done (e.g., monthly, weekly, or daily)?

Why it's important: Assessing the effectiveness of risk mitigation strategies helps the team identify areas for improvement and adjust their approach as needed.

Metrics to include: Incident reports, frequency and severity of incidents related to identified risks, and success rate of risk mitigation strategies.

Example: To mitigate the data breach risk identified in the previous question, the team may have implemented security protocols such as encryption and two-factor authentication. The effectiveness of these controls can be measured by analyzing the frequency and severity of incidents related to data breaches.

Are we in compliance with all laws and regulations applicable?

Why it's important: Compliance ensures legal and ethical business practices and prevents potential legal issues.

Metrics to include: Compliance audit results, frequency of compliance-related incidents, and success rate of corrective action plans.

Example: The team may be subject to regulations such as GDPR and PCI DSS. Compliance can be measured by conducting regular audits, assessing the frequency of compliance-related incidents, and tracking the success rate of corrective action plans.

How quickly are we able to respond to incidents, and how quickly are we able to mitigate them?

Why it's important: Timely incident response and mitigation prevent further damage and reduce downtime.

Metrics to include: Incident response time, time to resolution, and customer satisfaction with incident response.

Example: In the case of a data breach incident, the team's response time can be measured from the time of detection to the time of notification. The time to resolution can be measured from the time of notification to the time of resolution. And customer satisfaction can be measured through surveys and feedback.

What training and development opportunities are available to our team? "It's very important for us to continuously measure our team's level of training and development," Rajeev says. That includes keeping up with the product since product offerings often change.

Why it's important: Continuous training and development helps the team stay up to date with industry trends and best practices and improves their overall performance.

Metrics to include: Training completion rates, employee satisfaction with training programs, and performance improvement after training.

Example: The team may have access to training programs such as cybersecurity awareness training and agile development training. Completion rates and employee feedback can be used to measure the effectiveness of these programs.

What is our emergency plan? How would we respond to our worst-case scenario?

Why it's important: An emergency plan ensures the team is prepared to handle worst-case scenarios and minimize damage.

Metrics to include: Emergency plan documentation, frequency of emergency drills, and success rate of emergency response.

Example: The team's emergency plan may include protocols for responding to incidents such as natural disasters or system failures. The frequency of emergency drills can be measured, and the success rate of emergency response can be assessed through incident reports and customer feedback.

Key Takeaways

1. ***To build an effective team, consider four roles or mini-teams (KYC, AML, and EDD; transaction monitoring and customer sanction screening; fraud strategy and governance; fraud prevention and detection) and ensure team members possess curiosity, analytical problem-solving, attention to detail, and industry knowledge***

2. ***To justify the investment, link risk management to business goals, point to similar companies and their results, prioritize needs, and create a clear impact assessment***

3. ***To foster cross-departmental collaboration, set the tone from the top, share the same OKRs across teams, build relationships, and establish a compatible communication style***

4. ***To evaluate performance, ask questions about existing risks, the likelihood of occurrence, the effectiveness of mitigation, compliance with applicable laws and regulations, incident response and mitigation, and training and development opportunities for the team***

Successful fraud risk management is crucial to preventing and detecting financial crime, but it requires the right team, investments, cross-departmental collaboration, and performance metrics.

Q&A With Rajeev Muppala & Ali Rathod-Papier

Q:How does an organization's structure or industry affect its risk operations needs?

Rajeev:

Different industries carry different types of risks. For example, as a Fintech or a financial institution, your risk is different from someone that's focusing purely on technology solutions. Your obligations could differ by industry, country, and state, and you may need specialized risk management practices. You may need someone like Ali to be a BSA/AML officer because it's mandatory since you are operating in a regulated space.

I think we also need to look at our partnership ecosystem. Most of us in Fintech partner with a regulated entity like a bank that's offering services for us. It's very important for us to make sure that although we may be a modern Fintech or technology company, the back end is powered by a traditional bank. So, there are certain obligations that we need to fulfill, both in terms of third-party risk or reputation risk and regulatory compliance risk.

Ali:

Businesses are never static. Whether you are a small, fast-growing Fintech or you're a huge global financial institution, your products and services are going to change. The risk that you have in year one is probably going to be pretty different from what you have five years later. So, the organization has to have a structure to reassess and reevaluate its risk and figure out the new needs. Where you can go wrong is if you don't build that into your product lifecycle or your org changes. Your organization has moved on, but your program hasn't.

The second thing I'd say is it's good to take a step back and think about where you want your risk operations to sit. Do you want risk management to sit in the second line-of-defense team? Should it be part of compliance? Or do you want it to be in a first line-of-defense team? And I don't think that there is a right answer to that. I've seen it done both ways. I've seen it in compliance; I've seen it in the first line of defense. It's also worth understanding and acknowledging that

there are pros and cons to both and being very clear on why you are doing that, because I think that creates a delineated structure and makes people very clear on their own responsibilities.

Q: What are the essential roles within a risk operations team, and what attributes specifically would likely make them most successful?

Rajeev:

To build a successful risk ops team from a structural standpoint, you need to align on the key functions to focus on. Mine are KYC, AML, EDD (enhanced due diligence), etc.—that's one pillar. We also focus on screening. So, we have an obligation from transaction monitoring and customer sanction screening. That's another role that is very important in a risk ops team. And then we need fraud strategy and governance, which lead into your fraud prevention and detection.

These are the four key roles or key teams I think a risk ops team should have.

And in terms of the attributes that I would look for in a risk operations team, I think it's one—curiosity. You need to be curious as to what you're doing and also have good analytical problem-solving and attention-to-detail skills and industry knowledge.

Context is key because, most often, what happens is your analyst (or whoever's doing the job day-to-day) can read a procedure, follow the procedure, and still have bad money or money laundering happen on the platform. If you don't have the context, you're missing everything. Most of the alerts or transactions that we review, we have to review the type of account and expected activity. I think it's called contextual alerting. That is becoming a theme these days where it's not just based on certain rules, but it's actually based on a holistic approach.

Q: What KPIs are the most important for risk managers to look at regarding team performance?

Rajeev:

For the key performance indicators, we need to identify our risks. What risks do we have on the team or with the particular product? What is the probability and likelihood that these identified risks will actually happen? And then, how effectively are we mitigating these risks? Do we have controls in place? And how are we measuring those? Is it weekly reporting, monthly reporting, daily reporting? What is it? What kind of alerting do we get? And then we also should look at compliance. Are we complying with laws, regulations, etc.? Because that's another key performance indicator, in my opinion. You can have all the good fraud systems in place, but if you're not complying, then it all falls flat.

And then we will always have some issue or other that'll trigger an incident. An incident is basically a much larger issue—how quickly are we able to respond to this incident, and how quickly are we able to mitigate it?

One broad theme across all of this is training and development. **It's very important for us to continuously measure our team's level of training and development. Are they keeping pace with the times?** Are they keeping pace with, as Ali mentioned, changing products? For example, in Brex's five-year history, we have completely changed our product offering. We started as a credit card company, and now we are software as a service. So, has our team kept pace following this change, and are we now identifying the right risks? So, those are a few things that I would measure.

Ali:

I'd say two things to add on to that. Maybe I'm quite cynical in this respect, but I've seen in very large institutions that you have your KPIs, and you have your metrics, and they just become mindless numbers.

Bucket your risk into: what core areas do you have in your AML/OFAC program, how do your KPIs reflect that, and what metrics do you have related to it? And how does this information become useful? You also need to feed the information back into the program. It is pointless if you just churn through numbers and you have all of these KPIs, but then it doesn't inform your risk. And it's pointless if you don't keep recycling the knowledge that you gain from your metrics to make the program better.

Q: How do you approach justifying investment in risk operations to C-suite executives?

Ali:

The thing I've found to be effective in a Fintech is linking back to what the business wants to do. This banking partner is asking these questions, and if we don't respond, and we don't have a good answer, they're not going to work with us. And so, if the business can understand it as "these compliance things will be blockers if you don't do them," that tends to be quite effective.

And it's generally useful as well to point to similar companies in your space. "This Fintech just had this big fine, and they just got in a bunch of trouble. By the way, we looked at their consent order, and we have these issues. Do you think we should maybe do something about it?" Because I think having that real-life situation can help incentivize people.

Rajeev:

The way I pitch something like this to the C-suite is, "Hey, we want to unblock. We want to support you with your product. But these are a few things that we should absolutely do, and these are a few things that are nice to have." And on the definitely-do list, go with a clear-cut impact assessment. If the company does not do this, what happens? You could be fined; you could be barred from doing business in this jurisdiction. Appraise the leadership team of the business risks, regulatory risks,

and compliance risks that one may face in addition to losing money through fraud.

Compliance risk is always two, three years down the line, and most C-suites—especially in Fintech— may not have the foresight to see what's coming three years down the line. But financial loss is very immediate. You can feel it immediately, and you can fix it.

Q: How do you balance your risk and expenditure ratios?

Rajeev:

Part of this question is, how do we know enough is enough? **I mean, there will never be zero-risk tolerance ever.** If that's the case, then we don't need to be in business. We need to align on where we will fix and where we are willing to risk a loss. And that's why it's always a moving scale. It could change every month, it could change every quarter—depending on what kind of fraud pressure we are seeing during that time. You need to adapt every quarter, every six months. You need to be ahead of what the fraudster is trying to do or what the bad actor is trying to do.

Q: And what do you do if you find yourself in an organization that's resistant to investing in risk preparations?

Rajeev:

When you look at Fintechs or technology companies, it's always a trade-off. How much do you need to do here? Because you cannot have so many controls that it causes friction for your customer. In the Fintech space, the number-one mantra is zero friction for the customer, which is fine. But behind the scenes, how do we get comfortable from a compliance and fraud prevention standpoint? In a Fintech space, we typically find some resistance to deep investments in risk mitigation.

You have less convincing to do when it comes to fraud risk because if the company loses money, it will fix it. It's mainly on the compliance risk where the question becomes: why do we need to invest in this transaction monitoring? Why do we need to do the sanction screen? What's the big deal here? What happens if you

miss one? Because this is not an immediate impact. And I think this is where Ali and I are able to share anecdotes or real-life incidents from the past. This is where companies and management or boards that have discounted risk management have faced heavy burdens, terminations, and sometimes complete dissolution of the company itself.

Google it—you'll find thousands of examples where big banks have been fined, and how they've had to set up teams. HSBC, for example, had to set up 1,200 people in its AML function just because they didn't do something right. That's a huge burden. So, instead of resisting initial investment, it's better to invest and build this correctly so that we don't have to take a loss like this.

Ali:

This is a marathon, not a sprint. You're not looking for huge investments at the very beginning, and then it all goes away. Small, gradual investments over time can help. I completely agree with what Rajeev is saying. We have both experienced in Fintechs the resistance to investing in risk operations. That really challenges us as professionals to go back to some of the basics and identify the highest-risk item. You have 10 things to do, and you are telling the company you need to do 10 things, but they only have the money, staff, or enthusiasm to do five. What are those five things that have to be done? It challenges you as a professional to discover whether you truly understand what you're talking about.

You really have to think very carefully—do all of these 10 things really matter? Is this something you're going to lose sleep over, or is it going to be enough actually to do the five and still manage the risk?

That being said, I have sat in rooms with enough regulators during my time where I've thought maybe the five things or even the 10 things were enough, and it turns out they want 20. That can be the challenge sometimes. Regulators and examiners can have very strict interpretations of the law, of the regulation, and have very high standards. Even when

you are trying to be sensible and manage the risk, that risk-based approach doesn't necessarily translate that well in practice in an examination.

Q: What are the major blockers or challenges to cross-department collaboration when it comes to risk?

Ali:

Just speaking the same language. If you are working with teams that are not compliance experts (or don't really understand what it is you do), just translating it for them can be challenging. They have their own resource restraints, their own issues with investment. And so, you are not the only one who's saying, "We need you to do this thing." They have pressure from all sides. Making sure that you have a strong relationship communication style is helpful.

Rajeev:

In addition to what Ali mentioned, tone from the top when it comes to setting the OKRs. Because then you have cross-functional collaboration. You're looking at the same priorities, and multiple teams are invested in the same thing. Our priorities could be different when it comes to the day-to-day, but there also needs to be some aligned priorities. And that's what happens at Brex.

For example, we have a very good product team, and we have a separate risk and access team within the product team, where they collaborate with us day in and day out, with Ali and me. What should we look out for proactively? Ali, can you tell us if we need to look at this regulation or that regulation? From a fraud standpoint, what kind of fraud pressures will we see if we introduce this in this market? And the reason why we have been moderately successful is we both share the same OKRs. We have to answer to the same leaders.

Q: What kind of performance metrics are you looking at, and how do you use them?

Rajeev:

From a fraud standpoint, it's relatively easy because it's going to be a fraud loss performance. How much is the firm losing versus the risk appetite that you have set for the firm? When it comes to the compliance set of the house, the KYC side, this is where I ask what kind of metrics are okay. How are we coming across when we go through regulatory audits or audits from third parties? How are they rating us? Are we rating satisfactory? Are we not satisfactory?

Ali:

I completely agree with Rajeev. It's not just what are the day-to-day metrics you can say about how many customers you've onboarded, but what are your tests showing? On top of that, I think self-identified issues are even better because an audit or testing function is perhaps coming in with an external view of how the process works. And really, they're looking at the process and saying, "We've checked what you're doing against the process, and you're not exactly following what your process says."

Q: What do you think about the future of risk departments in modern organizations? Are they ready for evolving threats? What do you think the future of risk operations and risk management looks like?

Rajeev:

Are they ready for evolving threats? Yes, but we have to acknowledge the threats that we have in order to proactively mitigate them. I think that's where most organizations are reluctant. We all get newsletters from various companies that show emerging threats to compliance or fraud or whatnot. What do we do about it? Most often, it's just in a file somewhere. And only when you find something like the firm being in a consent order, for example, then you wake up. It's a wake-up call.

But on the positive side, I think there are also a lot of tools available in the market. Especially in the past five years, we have seen tens of hundreds of companies operate honestly in this space. Some will survive; some may not survive. But I've seen a lot of interest in companies building for compliance risk, fraud risk, and generally fincrime.

What I do not see is a good differentiation. Everyone says, “I’m the best.” Everyone says, “I’ll give you the least amount of alerts.” Everyone says, “Oh, you can integrate with me in no time.” The reality is completely different. And I think for someone to be successful here, it needs to go beyond promises, and it needs to go into how easy it is for last-mile integration.

Fraud Prevention: Your First Line of Defense

We've been on a long journey together.

We've discovered the ins and outs of spotting fraudsters, how they create identities, some of the tools they use, and the steps they take to manipulate people, infiltrate accounts, and commit nefarious acts, leaving behind damaged and broken lives in the process.

Now that we've come to the end, it's time to take action.

What do you do now that you've got this information? How will you lead your organization to get ahead of fraudsters? How will you become comfortable with sharing your stories to help others in the fight against financial crime?

It is an unfortunate truth that many fraud fighters are uneasy talking about their experiences for fear of exposing their competitive advantage to bad actors or bringing reputational repercussions to their organizations, but to be successful in this ever-evolving fraud landscape, cooperation is critical.

The first step to creating a successful risk management approach is simply to get comfortable recognizing and naming the threats out there and coming at them from a place of collaboration instead of fear.

"We have to acknowledge the threats that we have in order to proactively mitigate them," says Rajeev Muppala, the Head of Risk Operations at Brex. As we just saw with Rajeev Muppala's Q&A, he shared with us that many organizations are reluctant to act on emerging threats. "And only when you find something like the firm being in a consent order, for example, then you wake up. It's a wake-up call."

The wake-up calls that Rajeev is referring to would easily be avoided if more organizations were talking about the emerging threats they are seeing. Collective knowledge is the key missing ingredient from today's risk methodologies.

However, if we've learned anything on this adventure, it's that successful fraud prevention is a pairing of knowledge and following the best practices discussed in this book. As a recap, here are the things that you should keep in mind as you continue your fraud-fighting quest:

Be Adaptable

After considering the various approaches to fraud prevention presented by the experts we interviewed for this book, it is clear that flexibility is the key to preventing fraud in the future. “People tend to not have dynamic enough policies in place to stop fraud,” Robert Reynolds, Head of Product at Pinwheell, told us in Chapter 1. He reminded us that fraud adapts quickly, and the “set it and forget” mentality of thinking you can never fully solve fraud creates a false sense of security.

Fraudsters are a constant threat in today’s business world. They can take on many different forms and use a variety of methods to carry out their fraudulent activities. They may use phishing scams to obtain sensitive information, or they may create fake companies to defraud their victims. As the business landscape continues to develop new ways to prevent fraud, fraudsters are finding innovative ways to carry out their schemes. This means that fraud prevention programs must also be able to change as new threats emerge. In order to stay ahead of the curve, financial institutions must constantly evaluate current fraud prevention strategies and make adjustments as needed.

There is no one-size-fits-all approach to fighting financial crime. It can be challenging, and there are no universal solutions that work for all organizations. That being said, companies can take a multifaceted approach to protect themselves against financial crime. This approach entails working across departments to identify potential fraudulent activities and implementing measures to prevent them. A risk operations team will likely need to work with customer support teams, sales teams, engineering teams, and IT teams.

To effectively coordinate between departments, businesses must prioritize open communication and transparency to foster a culture of collaboration. This will require employees to develop skills in areas such as project management, communication, and conflict resolution. By investing in these skills, businesses will be better equipped to keep financial crime at bay and protect themselves against the financial and reputational damage that can result from fraudulent activities.

Buy Tools, Don't Make Them

Fraud prevention teams should be purchasing tools to help a team of risk management professionals instead of painstakingly building tools in-house that can completely automate risk prevention.

Buying software is a great way to keep your resources focused on your core business. When you build software from scratch, you often end up using a lot of time and money that could have been better spent on other important areas of your business. By buying software, you can take advantage of the expertise of the software vendors, and save yourself the hassle of having to develop, test, and debug software in-house.

Another advantage of buying software is scalability. When you buy software, you are often buying a product that has been designed to be scalable, meaning that it can grow with your business. This is especially important if you are an expanding business, as you want to ensure that the software you invest in can support your operations as they evolve. When you build software from scratch, you may find that it is difficult to scale it up on par with your business, which can lead to problems down the line.

The future of fraud detection and prevention are accessible and low-code solutions that enable a team of risk operations professionals to focus on—and succeed in—their work.

Keep the Human Element

Machine learning and data enrichment tools are great to have in your fraud prevention toolbox, but they are not cure-all solutions. Still, these tools are essential in today's world, where technology has made remarkable advancements, particularly in the field of risk management. Computers can process and analyze vast amounts of data, enabling them to identify patterns and calculate risk accurately. This capability has made them invaluable in risk management. However, despite their usefulness, computers possess limitations that cannot be overcome without human intervention.

Human experts have the critical thinking and analytical skills that computers lack. These skills include the ability to see the bigger picture and understand the greater context. And context is an essential component of sophisticated risk management, Rajeev told us in Chapter 6: "Context is key because, most often, what happens is your analyst (or whoever's doing the job day to day) can read a procedure, follow the procedure, and still have bad money or money laundering happen on the platform."

By combining the power of technology with human expertise and oversight, we can make more informed decisions which puts us at an advantage. Despite our mortal weaknesses, it's crucial to acknowledge the limitations of machines and maximize the strengths of humans while dealing with risk management. We can't stay ahead of the bad actors without both.

Fraud Is Not the "F" Word

Fraud is a serious issue that has become increasingly prevalent in recent years. It affects not only businesses but also individuals who fall victim to scams. It is essential to understand that fraud prevention goes beyond monetary losses. It is about protecting the people who are often hurt in many ways due to fraudulent activities. Fraud and money laundering are often linked to other crimes such as human trafficking, terrorist financing, romance scams, Ponzi schemes, and more. These crimes can have devastating effects on individuals and families and can effectively ruin lives.

As an industry, it is imperative that we work together to stop the fraudsters who are constantly collaborating and sharing information on how to scam and take advantage of people. Our best defense is to collaborate and share knowledge. This way, we can keep evolving our strategies to stay ahead of the game.

While tools are an essential part of the journey, it is the courageous people—the fraud fighters like you—who really make a difference in this fight. They care enough to work together to put bad actors behind bars and keep people safe. They are the ones who work tirelessly to investigate and prevent fraudulent activities.

Now that you've read the Fraud Fighters Manual, we hope that when you think of the word "fraud," you feel emotions of empowerment, optimism, and comradery instead of a flood of negative sentiments. We encourage you to share your own experiences and stories with us and others who may be going through similar situations.

Together, we can make a difference in the fight against fraud.

Unit21's No-Code Infrastructure for Fraud Prevention

Many customers come to Unit21 after experiencing issues with their former risk and compliance vendors. These customers are often seeking a more flexible solution that can meet their needs as they grow and scale. To address these concerns, Unit21 offers a comprehensive infrastructure designed to streamline risk and compliance operations and improve agent efficiency without writing a single line of code.

Unit21's no-code infrastructure allows for greater flexibility and quicker adjustments, as users can easily modify and test rules to further improve accuracy and reduce false positives as needed without requiring extensive technical expertise or engineering resources.

Unit21 contains an alert scoring system that gives teams insights about which alerts are the highest priority to investigate, and provides a single, centralized location for all of your data as well as the ability to visualize relationships between customers and entities through the use of network analysis. This gives agents a 360-degree view of their fraud detection program, and allows them to make informed decisions with ease.

Overall, Unit21 offers a comprehensive solution for risk and compliance management that is designed to meet the needs of modern organizations. Scan the QR code below to schedule a demo and see Unit21 in action:

Close your eyes, take a deep breath, and think about the word “fraud.” What comes to mind?