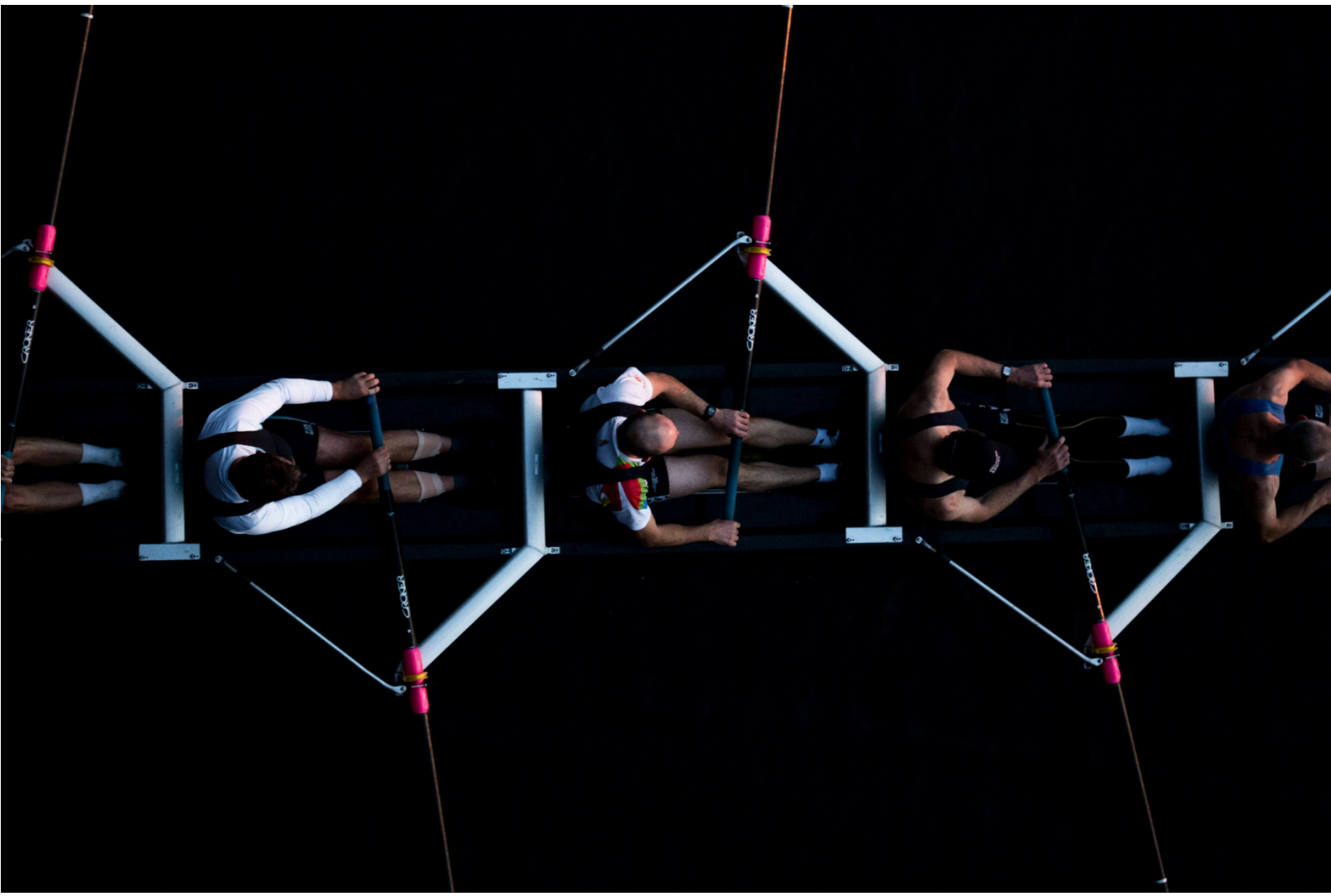


Improved Fraud Fighting Demands Greater Industry Collaboration

AMERICAN TRANSACTION PROCESSORS COALITION

atpc

GLENBROOK

Executive Summary

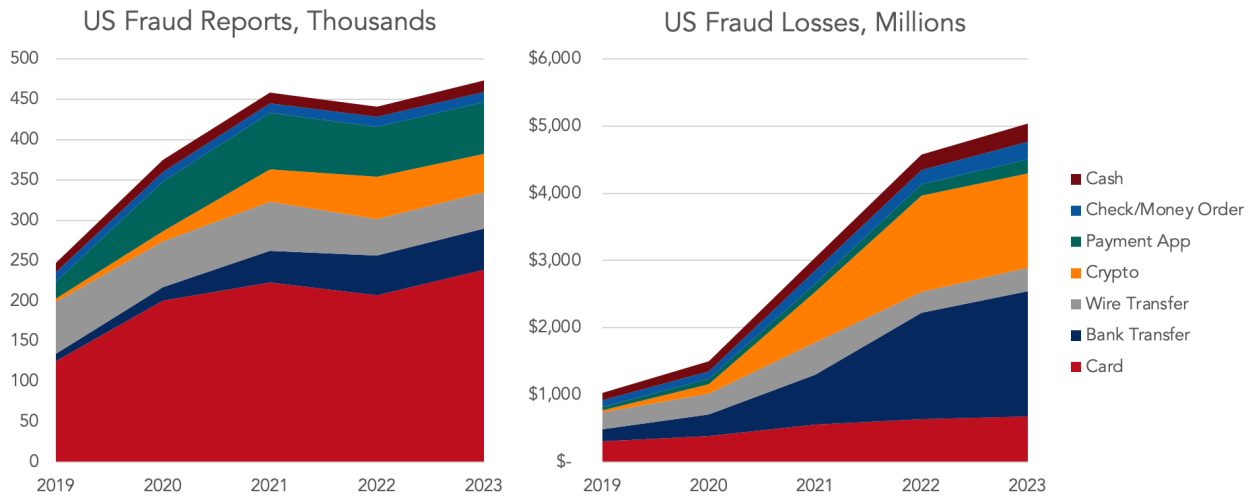
- Fraud is an increasing problem for the US payments industry, particularly in terms of the dollar value impacting consumer payments.
- Industry collaboration to fight fraud can be improved through expanded data sharing; this is particularly impactful as AI usage increases, offering ecosystem participants opportunities to leverage broader datasets to make informed decisions about transaction risk.
- Existing efforts to collaborate across stakeholder categories to reduce fraud demonstrate that coordination is challenging and that all stakeholder categories must have an equal voice to ensure success.
- Additionally, the US payments regulatory environment is fragmented and slow to respond to emerging payments risks, indicating an opportunity for greater dialog between payment industry stakeholders and regulators to ensure that regulations are clear, consistent, and responsive to new technological developments.

Current State		Ideal State
Data siloes preventing organizations from sharing information about potential fraud threats	▸	Real-time data sharing across stakeholders to facilitate faster identification of fraud threats
Limited industrywide collaboration to establish fraud mitigation strategies	▸	Collaboration between ecosystem participant categories to develop and implement new strategies
Fractured and reactive regulatory environment	▸	Ongoing dialog between regulators and industry leaders to establish holistic, harmonized guidelines

Fraud Is a Common Enemy in the Payments Space

We observe increasing instances of fraud across the payments value chain, an affront to the value of an industry dedicated to ensuring that electronic payments are secure and predictable. Fraud continues to hover at similar numbers year over year for incumbent payment systems, such as cards and ACH, and is accelerating for evolving payment methods, such as account-to-account (A2A), person-to-person (P2P), and digital wallet payments. Siloed mitigation strategies, driven mainly by liability holders, underpin this challenge. The industry can do more to drive cross-ecosystem collaboration, share necessary data, and define clear best practices and rules across emerging payment types. As leaders in the payments space, we must work together

to ensure that innovation can continue at pace without creating undue risk. But doing so has proved difficult to date, forcing us to reconsider how we can work together to limit the impact of fraud.



Source: FTC[1]

As the chart above indicates, while credit card fraud has remained stubbornly high, other methods of fraud in the US have increased dramatically in recent years. We observe instances of crypto and bank transfer fraud growing exponentially and the value of fraud losses to consumers ballooning in the aftermath of the pandemic. Although the FTC data shown above references consumer payments, fraud is a challenge across all participants in the payments ecosystem and all payment methods, and the definition of fraud has expanded to include a variety of maturing attack vectors that include scams, social engineering, and authorized push payments fraud. Fraud affects senders and receivers of funds, as well as their intermediaries. Fraud can impact consumers and businesses regardless of size, type, or industry. Fraud is global: While our core focus is the United States, we recognize that industry participants can be affected by fraud anywhere in the world, yielding lessons and insights for our specific fraud environment.

So How Big *Is* Fraud?

[1] FTC: "FTC Consumer Sentinel Network Data Book"

Payments fraud is a large and evidently growing problem in the US, but how large is it exactly? Reaching an estimate of the size of fraud requires answering a series of deductive questions. First, how are we defining size? Do we mean dollars, instances of fraud, or something else? Second, how are we defining fraud? For example, should our definition include scams or identity theft, which are often defined separately? Next, we must decide on a definition of "payments" fraud. Finally, to what group are we applying this definition of fraud? Consumers are probably more likely to disclose fraud losses than businesses, making it easier to arrive at a consumer estimate.

Let's answer those questions sequentially. First, we are interested in both the dollar amount of fraud and the number of instances. This allows us to understand size, incidence, and average value per incident. Second, we take a broad view of fraud, including scams and identity theft, as important drivers of phenomena like account takeover and synthetic ID usage. To qualify as payment-related fraud, fraud must involve a payment method or be enabled by a payment system. This, in turn, usually requires an identity associated with the payment account. This may be a borrowed identity (from a "mule"), a synthetic identity comprised of partially real and partially fictitious information, or a stolen legitimate identity. Finally, we are interested in both consumer and business fraud figures.

One significant source of data that satisfies three of our conditions is the FTC Consumer Sentinel Network Data Book.[2] The data book adheres to our broad definition of fraud. And while it also separates payment-related (or payment-enabled) fraud from other forms of fraud (e.g., employment fraud), it only pertains to consumers. Here, the FTC reports that consumers experienced $10 billion in fraud, approximately $5 billion of which was payment related. This $5 billion in losses were spread across more than 450,000 discreet complaints. So, we understand that this is the minimum value of fraud in the US, although some consumers may not report fraud and, more importantly, this value does not include business losses. Therefore, we must find another source to ensure we capture business fraud.

[2] FTC: "FTC Consumer Sentinel Network Data Book"

This often proves to be tricky, as businesses may be reluctant to disclose fraud events because they fear reputational damage. The Association of Certified Fraud Examiners (ACFE) estimates that businesses lose 5% of their revenues to fraud each year.[3] The US Census Bureau estimates that total US firm sales totaled $22 trillion in 2023.[4] If we apply the ACFE estimate of fraud losses to this figure, fraud would cost businesses more than $1 trillion each year. This is a huge number, representing almost 4% of US GDP, and is most likely an unrealistic estimate. Instead, to reach a more conservative estimate, we might draw from the FBI's IC3 reporting, which shows that businesses lost almost $3 *billion* in business email compromise attacks, across 21,000 incidents.[5] Again, this likely does not capture the full value of business fraud (particularly as it covers only a single vector), but it allows us to arrive at a defensible, conservative estimate. Indeed, the Association of Financial Professionals reported that 80% of treasury organizations encountered attempted or actual payments fraud in 2023.[6]

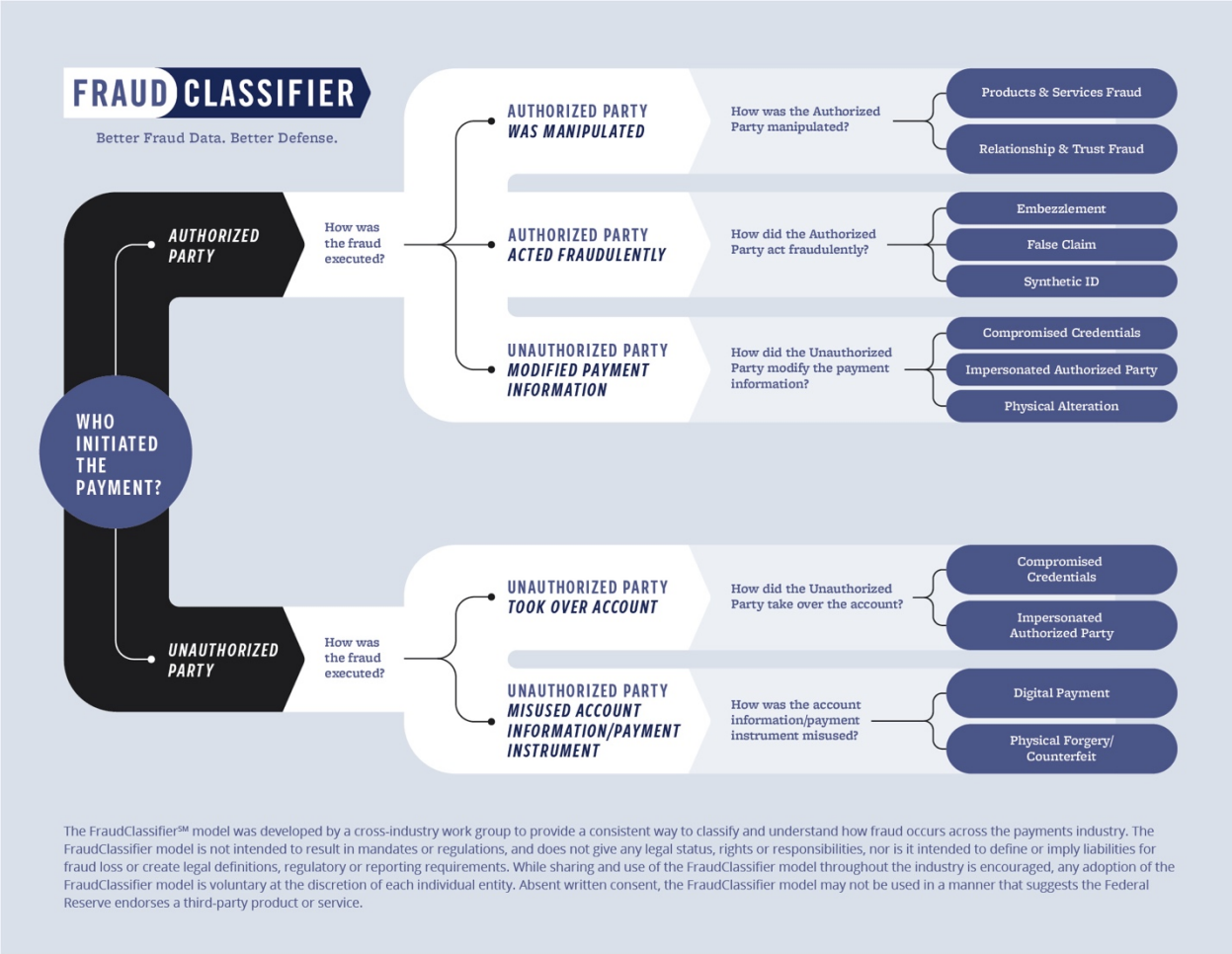
Based on publicly available information, we could reasonably state that the overall size of payments fraud in the US is ***at least*** **$8 bill**ion across almost 500,000 business and consumer incidents. But again, many incidents go unreported as individuals may be ashamed of becoming fraud victims, and businesses may fear reputational harm. That said, there are estimates of how much fraud goes unreported. We could arrive at a total fraud number by taking the estimated amount of unreported fraud and dividing our conservative estimate by this figure. For example, if 93% of fraud is unreported, the true value of fraud could be $8 billion divided by 7% (the share that *is* reported), or **up to $114 billion** across over 6 million incidents. We base this number on estimates of the share of unreported fraud from the FTC.[7]

To ascertain the accuracy of this number, we would need to also construct a "bottom-up" estimate, adding together different fraud types. Theoretical templates for this exist today, such as the FraudClassifier Model developed by the Federal Reserve's

---

[3] ACFE: "ACFE 2024 Report to the Nations"
[4] FRED: "Total Business Sales"
[5] FBI: "Internet Crime Report 2023"
[6] AFP: "Survey: 80% of Organizations Experienced Payments Fraud in 2023"
[7] FTC: "Protecting Older Consumers 2022-2023"

FedPayments Improvement group in 2020.[8] FraudClassifier aims to create a mutually exclusive and collectively exhaustive list of fraud types based on fraud attributes. First, was the incident initiated by an authorized or unauthorized party? Second, how was the fraud executed? The model yields twelve distinct fraud types, shown below.

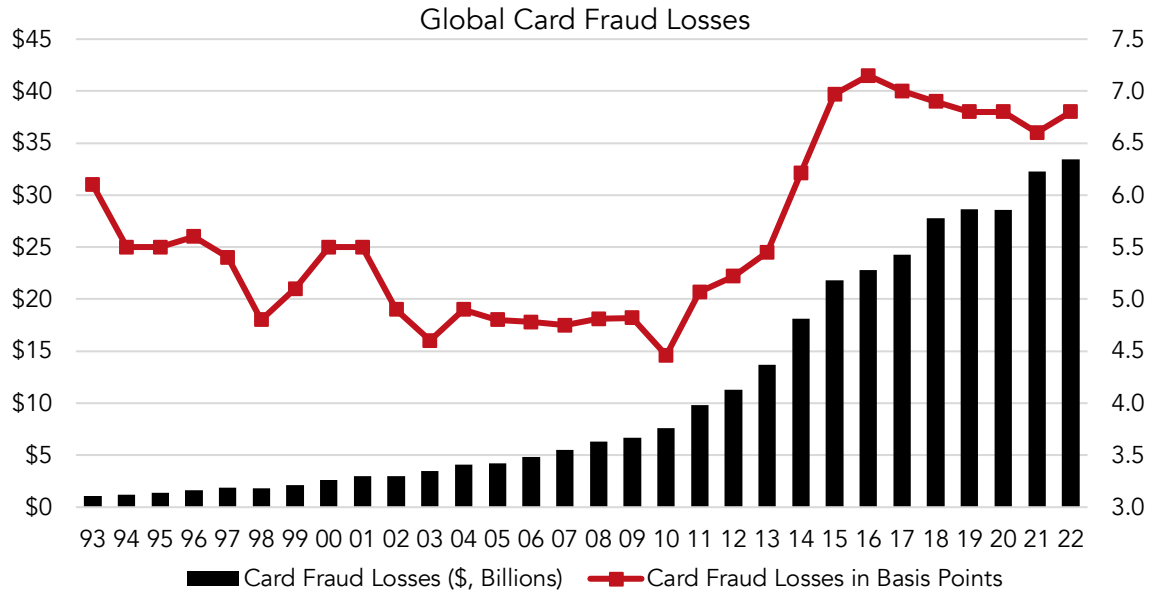


This is useful but does not solve the entire problem of arriving at a bulletproof estimate of fraud. As the Federal Reserve points out, the FraudClassifier Model's value comes from its implementation by industry stakeholders. Their adoption of the model would allow for standardized reporting across different payment types: ACH, card, fast payments, wires, checks, and even cash. This would allow industry observers to add together different kinds of fraud across different kinds of payments. However, it

[8] Federal Reserve FedPayments Improvement

requires coordinating reporting and publication of fraud data across the various entities responsible for each payment type (e.g., card networks, the Fed, and financial institutions). This level of industry coordination simply does not exist in the US today.

Existing Data Is Disjointed but Revealing



Source: Nilson Report[9]

While standardized reporting is not available, we can find evidence for the growth of fraud in some available data. For example. the card environment is a useful case study in the evolution of payments fraud, particularly in the US where cards are a prevalent form of payment. The overall value of fraud continues to grow, which is to be expected as the overall volume grows. However, we have also seen the percentage of fraud continue to increase over the course of the past decade. Card fraud can scale as the overall card environment scales because fraudsters adopt new technologies and approaches. For example, card not present (CNP) fraud now accounts for 74% of all US card fraud losses, up from 57% in 2019, representing $10.6 billion, driven by a boom in e-commerce already underway and accelerated by pandemic lockdowns and resulting consumer behavior shifts[10]. The shift to CNP fraud

[9] Nilson Report, December 2023 Issue
[10] EMarketer/Insider Intelligence: "US Total Card-Not-Present (CNP) Fraud Loss, 2019-2024"

highlights' fraudsters' adaptability to new market paradigms and the ability to do it in a fast and responsive way with a level of effectiveness that we have not seen in the past.

Fraud is also increasing in the ACH environment, where transactions take place digitally by design, in many cases displacing volume that in the past would have been conducted by check. As ACH transactions grew from 25 billion in 2019 to 32 billion in 2023, representing $80 trillion in value, fraud has become top of mind for organizations participating in the network.[11] A recent AFP/J.P. Morgan study found that 30% of organizations observed fraud involving the ACH system in 2022. While the number of organizations noting fraud via ACH debits decreased year-over-year, organizations report that fraud via ACH credits, including Zelle, increased by 6%.[12] Even checks – perhaps the oldest of modern payment methods aside from cash – have experienced a resurgence in fraud losses, despite their significant decline in utilization among both consumers and businesses.[1]

Indeed, fraudsters are savvy innovators who thrive in the digital era, scaling their operations and revising their approaches to match the overall ecosystem.

Fraud Innovates

Fraudsters follow fintech and payments trends as closely as we do because they understand an unfortunate reality of technological progress: As new technologies are deployed and new businesses are created around them, new opportunities for fraud emerge. As "traditional" payment methods like cards and ACH adapt to a digital, connected world, novel faster payment methods like FedNow, RTP, and Zelle have emerged. For businesses and consumers alike, fast payments represent a meaningful improvement for end users. Funds move immediately, in real-time, outside business hours, and are irrevocable. These factors improve trust in the new payments systems as senders and receivers immediately know if a payment succeeded or failed. Immediate funds access can meaningfully impact consumers (through earned wage access or fast claims disbursement) and offer working capital benefits to businesses.

---

[11] Nacha: "ACH Network Volume and Value Statistics"

[12] AFP/J.P. Morgan: "Payments Fraud and Control Survey Report"

However, the same factors that make these novel payments systems attractive to end users and the providers that serve them also make them attractive to fraudsters. Furthermore, fintech innovation and evolution often provide criminals with a greenfield opportunity to exploit immature processes, controls, and new payment paradigms that have not had the same level of scrutiny that incumbent payment systems have undergone over several decades.

Fraudsters value the speed and finality of these transactions, especially in impersonation scams. Posing as a new friend, romantic partner, financial advisor, client, or marketplace buyer, or otherwise gaining the trust of another user on the internet (like over a messaging app or via email). After building trust over the course of hours, days, weeks, or longer, these fraudsters "seal the deal" with a payment request. When the victim obliges, money moves instantly and cannot be reversed.

The FTC estimated that these relationship schemes, of which evolving payment technology is an essential component, cost Americans $1.4 billion in 2023. That number will likely continue to rise in 2024.[13] Regulators are concerned: In 2023, Senator Elizabeth Warren and others questioned banks' ability to adequately protect their customers from scammers. Against this backdrop, Zelle's operators codified rules that allow for consumer fraud reimbursement following imposter scams[14]. Will it be enough to deter fraudsters? Or will they find new avenues to attack vulnerable Americans? Fraudsters' quick adoption of fast payments encapsulates the problem of fraud following payments innovation and demonstrates that the latter is the more likely outcome.

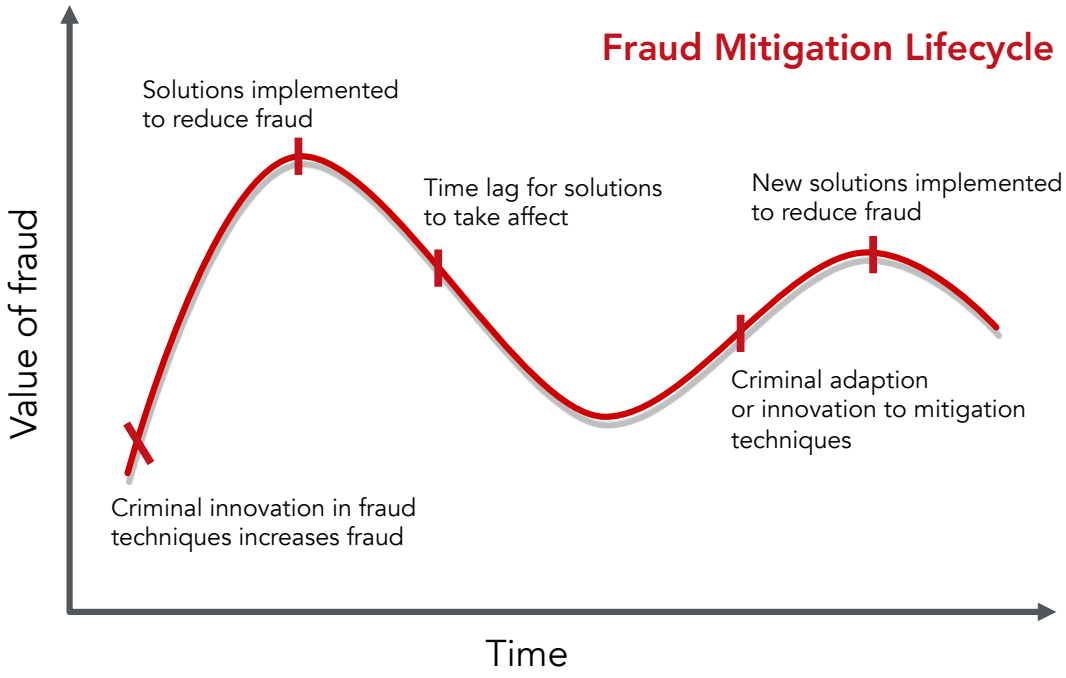
Today's Fraudsters Seek Gaps Opportunistically

As new technologies emerge, the payments industry introduces new risk mitigation tools. Subsequently, fraudsters adapt to these fraud mitigation techniques. In response, the payments industry adapts to fraudsters' new approaches. The resulting "arms race" results in a fraud control lifecycle that sees ongoing peaks and valleys in

[13] FTC: "As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public"

[14] Reuters: "Payments app Zelle begins refunds for imposter scams after Washington pressure"

fraud rates as fraudsters innovate and the industry reacts. However, we are concerned that the industry's ability to address new attacks may struggle to keep up with the rate at which fraudsters introduce new techniques. Fraudster adoption of AI is particularly concerning. AI allows fraudsters to launch larger attacks more frequently, learn from the results of their attack, and adapt to evolving risk mitigation strategies in near real-time.



Source: Glenbrook Analysis

In addition to leveraging new payment technology to find new avenues for attacks, fraudsters are adopting new computing approaches and organizational capabilities to facilitate additional opportunities. In many respects, they look like private companies in their structure, services, and innovative approach, contributing to the emergence of a "fraud industry." Some key strategies that are increasing the scale and effectiveness of modern-day fraud attacks include:

- **Fraud-as-a-Service:** Fraudsters have established a business environment in which specialized actors collaborate with others to provide services, expanding their clients' capabilities and reach. This enables criminals to adopt more sophisticated fraud techniques and scale their operations more

efficiently than they have been able to in the past. As individual actors in the fraud-as-a-service space introduce new features and capabilities, the entire "fraud industry" increases its collective capabilities.

- **Big Data Capabilities:** As stolen records are increasingly available on the dark web, fraudsters can collect information and piece together consumer and business profiles, allowing them to access sensitive information or create new accounts. In 2023, 17 billion records were exposed, a 35% increase year-over-year.[15] That data will be ingested by fraudsters to augment their existing collections of personal information, enabling more sophisticated and targeted attacks.
- **Generative AI in Fraud:** Fraudsters now leverage generative AI to accelerate their data collation activities and realistically create new synthetic identities. This latest generation of AI technology can help fraudsters scale automated operations more efficiently. This can range from creating realistic digital identities to thwart transactional and account fraud detection systems, to highly sophisticated document generation systems that produce realistic passports and driver's licenses.

Synthetic identity fraud is a worrisome and pervasive development in this space. Fraudsters scour the internet and the dark web for personal details to stitch together customer profiles, imitating real people or entities or fabricating entirely new ones. Few organizations can identify these, making the vast majority of ecosystem participants reliant on third parties. Greater collaboration and data sharing across the large, sophisticated providers of third-party synthetic identity risk mitigation tools can help our industry fight ever-innovating fraudsters.

While this sort of "professionalized" fraud is both significant and alarming, its emergence does not mean that more "entrepreneurial" forms of digital payments fraud have died off. On the contrary, payments organizations increasingly contend with fraud perpetrated at the individual level. Returns fraud, policy abuse, and first-party fraud have hit new highs and are now the #1 concern among merchants.[16]

[15] Infosecurity Magazine: "17 Billion Personal Records Exposed in Data Breaches in 2023"
[16] Cybersource: "2024 Global Fraud and Payments Report"

In both cases of professional and individual fraud, we observe bad actors finding and exploiting the control gaps that accompany the introduction of new technologies and business processes. This further demonstrates a need for greater industry cooperation to prepare and preempt the risk challenges inherent to technological advancement in the payments ecosystem.

Fraud Is an Industry Problem

Looking forward, we start from the premise of two intertwined but distinct invariants shaping fraud detection and mitigation in the payments industry. First, we understand innovation is a vital component of the payments landscape – innovation allows the payments industry to meet evolving consumer preferences and to generally deliver more efficient, lower cost services. At the same time, these new innovations also attract new types of fraud, now perpetrated by ever savvier and more professional fraudsters.

Nevertheless, we observe that the industry's fraud-fighting approaches are fractured at a time when broader, more collaborative approaches will yield more effective results, particularly as AI enables ecosystem participants to make decisions with larger sets of data. However, a few key drivers perpetuate a fragmented response to fraud.

The existing structure of regulatory and financial liability contributes to this fragmentation. Many providers are concerned primarily (or solely) with their specific stage of the transaction lifecycle: They are concerned with preventing fraud as payments transit through their environment but have no reason, from a liability perspective, to care if the same transaction proves to be fraudulent at another stage of the journey. This impedes effective risk mitigation, as a provider may pick up a signal that could help inform a downstream party of a potential risk but is not incentivized to share this information.

Individual providers aside, there are also impediments at the network level. Payment networks and system operators could theoretically "see" across their entire networks to inform participants of fraud patterns that could enable better risk detection at the

provider, current data-sharing arrangements do not support this. While RTP and FedNow can share information about confirmed and suspected fraud, individual participants or providers must piece together fraud patterns.[17, 18] Although Nacha recently issued new rules requiring promoting fraud detection in credit-push transactions, the onus to do so remains on individual liability holders.[19] Elsewhere, as in the card network, data is shared selectively, limiting its effectiveness. Network participants can enroll in a patchwork of programs or pay for access to decision-making intelligence, but the result is a space that many fraudsters—through a combination of savvy, perseverance, and luck—can weave through undetected.

This is not to say that there haven't been industry efforts to get multiple parties to "speak the same language" and align toward higher levels of fraud detection. A notable effort by technology providers, including Mastercard and Visa (and now managed by EMVCo), dating back to the early days of e-commerce is the 3-D Secure (3DS) protocol for CNP transactions. The "3-D" here refers to the three domains involved in a 3DS transaction: the e-commerce merchant, the online consumer, and their issuing bank. In a 3DS transaction, cardholders are asked to authenticate themselves (e.g., via their banking app) as part of the payment flow.

In the latest version of the protocol, available since 2016, consumers are only required to authenticate if they or their transaction meets certain criteria; that is to say, the transaction appears to be riskier than usual. This change to the protocol reflects the fact that trying to coordinate consumer behavior, issuer user experiences, and merchant implementation led to consumer frustration and, in turn, checkout abandonment. But even in this revised version of the protocol, users are routed down the authentication path. To make matters worse, merchants generally do not have visibility into the factors that led their customers to be asked for authentication.

[17] The Clearing House: "RTP Operating Rules"
[18] Federal Reserve Financial Services: "Protecting Against Instant Payment Fraud"
[19] Nacha: "New Nacha Rules Take Aim at Credit-Push Fraud "

Furthermore, the lack of data standardization and decisioning practices across the ecosystem has led to a chicken-end-egg problem when it comes to the adoption of 3DS within non-regulated geographies. Merchants often note that their use of 3DS is limited because issuers' authentication decision processes are inconsistent and inconvenient to consumers. However, when issuers are asked why they are not investing in more sophisticated authentication practices, they often state that merchant utilization of the protocol has been limited. As a result, 3DS adoption remains very low outside of markets where it is required by local regulation.[20] Any future solution must provide merchants with a code to explain why additional verification is required. Then merchants would be empowered to explain to customers that a security concern has been identified and the additional step is for their own protection.

Clearly, whether as a result of siloed data sources or clunky processes that attempt to speak across disparate groups, our efforts to mitigate fraud through industry-wide collaboration have been ineffective. Yet even here, we see the challenges presented by the current protocol as an opportunity: There are avenues to improve 3DS to ensure that its vision of collaborative fraud fighting is not lost. By increasing dialog between various stakeholder categories (networks, issuers, merchants, and consumer advocates), the industry can improve the 3DS experience and increase usage to e-commerce fraud. Such efforts could include greater data standardization in merchant data, clearer rules and guidelines related to the protocol itself, and performance benchmarks for issuers. 3DS points towards a more involved, collaborative approach to risk mitigation.

3-D Secure adoption in unregulated geographies, such as the US, could greatly benefit from stronger collaboration and alignment of best practices across all parties within the payments ecosystem. Improvements that could move the needle in both adoption and performance include:

- Requirements to use consistent enhanced data sets for each transaction

[20] Glenbrook Partners: "A Merchant's Guide to Assessing 3-D Secure"

- Development of modern best practices for all participants, including merchants, merchant 3DS plugin providers, issuers authentication system (ACS) providers, and issuers
- Implementation of required performance thresholds for issuers, including overall approval rate requirements
- A requirement for issuers to utilize authentication systems that rely on modern decision technologies, with a heavy focus on adaptive machine learning
- Greater collaboration between standards bodies, card networks, and technology providers to standardize best-in-class technologies required to address conversion and detection shortcomings

Our Regulatory Environment Presents Challenges and Opportunities

Another area of opportunity for greater collaboration is the regulatory space. In the US, regulation of the payments space is often murky, which can lead to unintended consequences. To ensure that regulation is clear, consistent, and adaptable, payments leaders and regulators can improve communications around new technology, new threats, and industry efforts to reduce fraud.

The challenge stems, at least partially, from the fractured nature of the regulatory landscape. The US lacks a single payment regulator or policy maker, and we have seen payments regulation set by Congress, the Consumer Financial Protection Bureau, the Federal Reserve, the FTC, individual states, and others. There is no consolidated payment body or vision regarding payment regulation in the US. This diffuse landscape contrasts the approach taken by other regions, such as the UK, the EU, and Australia, where payments regulation is more clearly defined and centralized. But even if a centralized payments regulatory regime were established, it would likely struggle to adapt to a shifting fraud battlefield as the payments ecosystem evolves.

Take, for example, the challenges the Payment Services Regulator has faced in the UK. Fast payments, for reasons discussed in our earlier description of the benefits of these payment types to scammers, have led to a meteoric rise in authorized push payment (APP) fraud. The regulatory body has moved to quell consumer losses by requiring mandatory reimbursement from financial institutions for consumers

affected by APP fraud[21]. While this encourages better controls among banks participating in the fast payments space, it does not address the root causes of the scams themselves or even facilitate data sharing to identify fraud patterns across providers. As a result, fast payments may come to be seen as a cost to be managed rather than an innovation opportunity for financial institutions. Early participants in the card system struggled with a similar challenge before the space matured.

Regulatory Maturity Model

Liability Rules Defined → Regulatory Frameworks in Place → Data Sharing Facilitated

In the US, we see similar challenges: regulations follow fraud behavior, which can evolve rapidly. As we noted earlier, fraudsters are highly opportunistic, but regulatory diffusion does not help this problem. We lack clear rules around liability in emerging payments systems like Zelle, for example, and even in established systems (e.g., card networks), liability rules are set by networks rather than any regulatory body.

Going a step further, we lack full regulatory frameworks for emerging payment types and struggle to incorporate technological advancement into existing frameworks. The Federal Reserve has clarified Regulation E, which had most recently been modified to address unauthorized push payment fraud but not authorized push payment fraud. In November 2023, the CFPB proposed new rules regulating tech companies offering bank-like services along the same lines as banks and credit unions[22]. However, the US generally does not have an established method for determining when a new payment method or fintech product has become systemically important. Regulators will most likely grapple with this issue in the coming years and decide what level of regulation must be enforced on non-bank entities, especially those providing novel payments and bank-like services.

Putting aside liability clarifications, regulatory frameworks, and an ability to keep pace with rapidly evolving technology, a highly sophisticated regulatory apparatus would

[21] Reuters: "APP fraud: The UK's mandatory reimbursement requirement"

[22] CFPB: "CFPB Proposes New Federal Oversight of Big Tech Companies and Other Providers of Digital Wallets and Payment Apps"

require data sharing across payments providers and payment types (both to ascertain the true size of fraud and to develop strategies to prevent its growth) and could even incorporate data from beyond the payments space.

In what was a surprise development to many, European regulators have very recently recognized that cross-industry data sharing is critical to effective fraud collaboration, proposing a regulatory data sharing framework as part of the proposed Payment System Directive version 3 (PSD3) and Payment System Regulation (PSR)[23]. In India, the central bank is exploring ways to integrate new technologies for fraud detection into the Unified Payments Interface system.[24] In the US, industry leaders can influence how any regulatory action could define new standards of minimum viable fraud-fighting and incentivize data-sharing. This is an exciting opportunity to work collaboratively with regulatory stakeholders to shape future interventions that challenge the existing fractured and reactive regulatory paradigm.

INDUSTRY PARTICIPANTS MUST ACT

Continued innovation in the U S payments industry benefits new and established businesses, consumers, and government—with significant impact on the nation's economy. However, many potential benefits accruing from high-potential innovations are curtailed because of rampant and growing fraud throughout the payment industry.

The challenges of fraud are shared across the industry ecosystem. Remedies are not.

The mechanisms, practices, and tools for sharing details of instances of fraud as well as real-time fraud trend data are minimal, at best. In addition, fractured regulatory structures impede industry efforts to collaborate in ways that would mitigate and measurably reduce fraud.

To address the growing fraud crisis, the American Transaction Processing Association (ATPC) proposes four essential and viable initiatives.

1. **Standardize and Share Fraud Data**

[23] DLA Piper: "PSD3 and PSR: sharing data on fraudulent payment transactions"
[24] The Economic Times: "RBI's proposed digital payments intelligence platform will mitigate frauds, say experts"

Standardize data sharing at the network level and within payment methods, including payment cards (debit, credit, and prepaid), the Automated Clearing House (ACH) and for instant payments, including Real Time Payments and Fed Now.

Precedent for standards establishment is evident in the EMVCo payment card standard established by Europay, Mastercard and Visa (EMV) for card network participants. The widely adopted standard is now managed by EMVCo, a consortium with control split equally among Visa, Mastercard, JCB, American Express, China UnionPay, and Discover.

~~2.~~ **Leverage Artificial Intelligence Technology**
Support and facilitate use of artificial intelligence (AI) technology enabling payment participants and providers to absorb large data sets, using them to improve fraud-related detection and rejection decisions. Given the adoption of AI, collaboration among participants in the ecosystem can reduce their vulnerability from fraudsters.

Artificial intelligence technology includes machine learning and its subcomponents of neural networks, deep learning, large language models, and generative AI. Their use is skyrocketing and can be leveraged within the payments ecosystem. *Time is of the essence* as fraudsters are also adopting AI technology at a rapid and accelerating pace.

3. **Convene Payment Industry Working Groups**
Initiate working groups comprised of payment company representatives to identify, prioritize, and implement data sharing practices according to agreed upon standards (from initiative 1). There are sufficient precedent-setting instances of this. The most recent is card issuer Capital One's announced collaborative effort with payment service providers (PSP) Stripe and Adyen. Their collaboration enables instances of fraud observed by one participant to be used in the others' risk decisions.

4. **Advance Industry, Regulatory and Legislative Collaboration**
Establish a mechanism for timely collaboration and direct communication between the industry's policy-making institutions and both legislative rule-making and regulatory bodies. Frequently payment ecosystem participants are forced to confront emerging issues, whether potential opportunities or distinct problems, without clear guidance on viable actions or responses. These challenges can be eliminated by a focused collaboration initiative. Potential models have been established by the European Union (EU) with Payment System Directives 2 and 3 and the EU Payment Services Regulation (PSR).

It is well understood that fraud in the payment industry ecosystem is a never-ending challenge, and one where fraudsters are ever-more clever and innovative. The U S payment

industry must step up its efforts to deal with the challenge through the initiatives that have been outlined. *The time to act is now.*