Deloitte.

P2P Fraud Challenge: Mitigating Risk in a Changing Digital and Regulatory Landscape

Deloitte Risk & Financial Advisory Point-of-View
March 2023

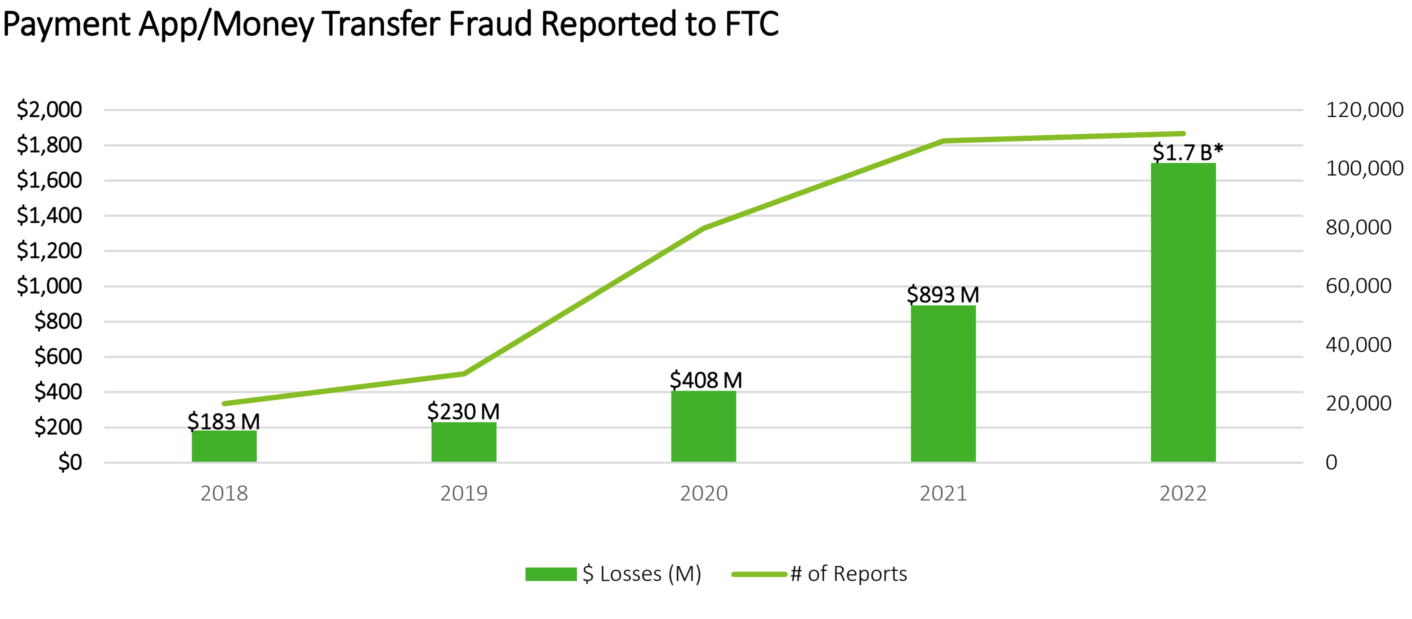
MAKING AN IMPACT THAT MATTERS since 1845

Introduction

The peer-to-peer (P2P) payments/money transfer industry is experiencing a consistent year-over-year increase in fraud losses, **with 2022 projected to end with a 90% increase over 2021 at $1.7B** and a nearly ten-fold increase when compared with 2018[1]. This is driven by both the increased consumer adoption of P2P payments as well as the increased prevalence and sophistication of first and third-party fraud schemes. Along with pressures from mounting fraud losses, financial firms are facing increasing pressure to compensate victims of P2P fraud claims.

Figure 1. FTC Reported Losses[1]

Data captured from FTC consumer-reported payment app and money transfer losses from 2018-2022 shows a strong upward trend in both monetary losses and total number of reports.



**2022 projection is based on Q1-Q3 FTC reported data*

Source: Deloitte analysis of FTC Fraud Reports data

Background

P2P transactions are gaining popularity and a growing number of banks and fintechs are entering the payment space. These firms have attracted customers by offering easy-to-use mobile apps, minimal transfer fees (often no fees for transfers under certain dollar thresholds), and instant funds availability. P2P activity has seen substantial growth in the past year with 118.3 billion real-time payments made across the globe in 2021, a year-on-year growth of 64.5%[2]. While banks and fintechs are offering increasingly frictionless methods of moving money, the US Consumer Financial Protection Bureau is pursuing enhanced regulatory guidance to improve customer protection.

The efficiency of digital payments presents a unique problem for P2P providers – while providing the customer with an immediate money transfer experience, it can also enable bad actors with an expedient means for extracting money from customers and accounts. Common schemes used by bad actors typically fall into two main categories: fraud & scams.

Fraudulent transactions are those generally initiated by individuals who **are not the actual customer**, but who have obtained control of accounts, credentials, identities, etc. to access and initiate transactions.

Scams generally include transactions that **are authorized by the customer themselves;** but in these cases, the customer has unknowingly been “duped” into agreeing to transfer funds.

With the evolution of the expectations on how institutions compensate customers for digital payments fraud, it has become increasingly important for P2P providers to leverage muti-layered detection methods to proactively identify fraud and scams throughout the payment lifecycle. The breadth of the scam problem is extensive. The top five fraud loss categories reported by the FTC in 2021 were primarily scam-related, including: imposter scams ($2.3 billion); online shopping scams ($392 million); prizes, sweepstakes, and lotteries ($263 million); internet services ($223 million); and business and job opportunities ($209 million)[3].

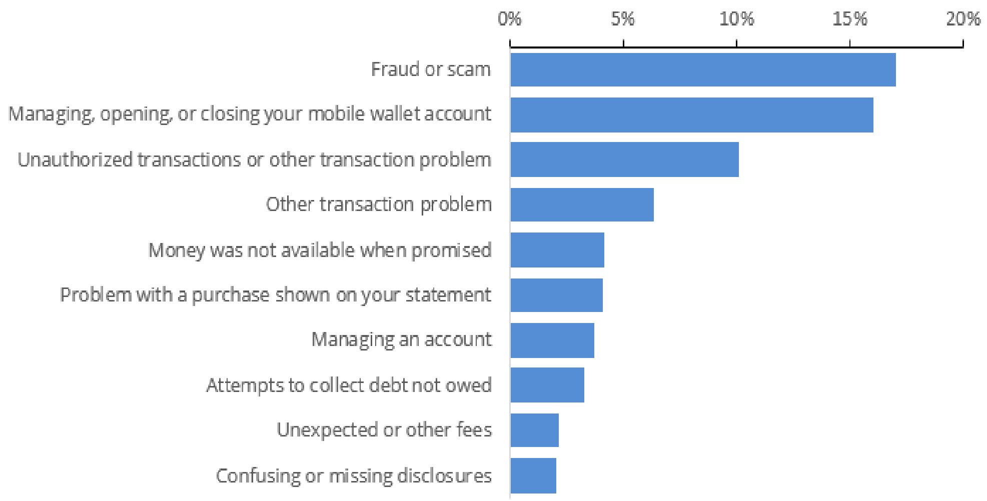
Regulatory Scrutiny

Historically, banks have covered consumer losses for victims of third-party-induced fraud. However, the evolving payments landscape is making it difficult for regulators to distinguish which financial institution is responsible for scam victims. In December 2021 the Consumer Financial Protection Bureau (CFPB) indicated potential changes to Reg E to compel banks to reimburse victims’ P2P payment scam losses[4]’ [5]. Under current Reg E guidance, banks will only reimburse consumers for losses on P2P transfers when they’re “initiated by a person other than the consumer without actual authority to initiate the transfer,” which allows banks to deny reimbursement for consumers who initiate the payments themselves[6]. In response to the changing regulatory landscape and consumer expectations, banks have recently begun working to cover P2P scam losses as well.

Figure 2. Insights From CFPB Complaints Data

Text analysis conducted on CFPB consumer complaints data for top payment app providers shows fraud or scam-related complaints making up the largest proportion of complaints from 2020 to 2022.

Top P2P Provider Complaint



Source: Deloitte analysis of CFPB Consumer Complaint Database

Data Insights

164%

Increase in monthly average complaints for money transfer services in 2021 versus previous two years[7]

41%

Of complaints closed with explanation or relief were fraud or scam issues[7]

The Shifting Landscape

With new payment rails and P2P services poised for growth, there are some fraud and scam types that are evolving. Holistic countermeasures need to move beyond transaction-centric detection.

Fraud

With the increasing prevalence of personally identifiable information (PII) compromises throughout the industry, fraudsters have troves of identity data available to them on dark web exchanges which they can use to open new accounts or take over existing accounts. Over the past decade, the five largest publicly reported data breaches ranked by number of social security numbers impacted resulted in the cumulative compromise of more than 1.3 billion PII records[8]. Fraud detection strategies developed for scams are often very similar compared to those targeting identity fraud. These strategies should consider the organization’s ability to service and leverage modern technologies like device fingerprinting, behavioral biometrics, third-party PII risk modeling, and anomalous transaction behavior modeling.

Account onboarding is a consistent challenge to institutions because it involves a limited set of verification indicators, typically Government ID, SSN, address, phone number, and email address. Through the litany of large-scale data breaches across the industry, this information is readily available to bad actors. In response, some institutions have taken an enhanced layered detection approach to new customer validation and have incorporated new technologies like PII risk models, email risk scoring, selfie information (which can be used for both facial recognition and device profiling), and customer profile AI/ML models.

Fraud Application

If fraudsters can’t defraud a victim into authorizing a transaction, they can resort to account takeover (ATO) tactics and breach the victim’s account themselves. This will often involve fraudsters phishing for account information or purchasing customer PII on the dark web. Layered detection strategies are particularly helpful in this area, as previous good customer transaction activity and device interactions can be leveraged to detect anomalous behavior that may indicate a bad actor has taken control of the account. Integrated detection systems play a critical role in this area as they enable the utilization of cross-lifecycle detection strategies.

Account Takeover

Scams

The nature of scams is constantly evolving due to consumer awareness, new technologies, and risks with new product offerings.

Investment Scams: This is one of the fastest growing scam types, wherein fraudsters will convince victims to transfer money to buy stakes in crypto, NFTs, and other digital investments. The FTC reported over $1 billion in losses for crypto-related fraud in 2021, a 6,000% increase compared to 2018[9]. Despite the risks inherent in the crypto-currency space, many P2P providers are rolling out crypto-wallet capabilities. The FTC also noted that consumers of ages 20 to 49 were more than three times as likely as older age groups to have reported scam losses from cryptocurrency payments[9].

Elder Scams: A consistent target for fraudsters has been elderly consumers, who are often less technologically savvy and more susceptible to fraud schemes. According to the FTC's 2021 fraud loss data, of the $518 million total reported fraud losses by consumers aged 70 years or older, a vast majority was attributed to scam-related fraud[1]. The largest categories include: romance scams ($94 million); prizes, sweepstakes, and lotteries ($90 million); business imposters ($80 million); government imposters ($60 million); and tech support scams ($47 million)[1]. Additionally, the median loss reported by consumers in elderly age brackets was two to three times higher than consumers in lower age brackets[1].

Mitigation Considerations

Considering fraud evolution coupled with the increase of threat, fraud event velocities, and technological advances (i.e., machine learning, device identification, and behavioral biometrics), organizations need to have an effective triage approach that prevents, detects, and remediates the various fraud risks. There are heightened consumer expectations with regards to fraud liability.

Governance:

Robust fraud management governance structures like fraud risk management committees, operational oversight committees, and effective documentation provide greater transparency as expected by the regulators. Comprehensive fraud policies and standards can include transaction monitoring, real-time detections, customer authentication, fraud case reviews, robust root cause analysis, and machine learning feedback loops. Establishing a strong fraud risk culture coupled with effective fraud governance controls and policies go beyond regulatory compliance.

Technology:

Leveraging new technology like behavioral analytics utilizing machine learning, advanced analytics, geolocation, and geo-velocity, can enhance authentication security and help to continuously refine the picture of the user. Below are some recent technologies that are gaining adoption across the industry:

Device Fingerprinting: Leveraging location (GPS & IP), DSN, telemetric, and device fingerprinting data to build customer profile and detect anomaly indicators to compare against previously flagged devices and IP addresses.

PII Risk Models: Some third-party tools now offer high-risk customer PII indicators and risk scoring for information like name, address, SSN, and email to detect new, frequently used, and previously flagged customer information. This information can be used to flag high-risk account openings and input into customer profile monitoring to aid in transaction detection and customer servicing.

Passive Biometrics: Leveraging device behavioral information collected through customer in-app and web interactions enables issuers to quickly spot anomalous behavior during account access and servicing. This data is collected during the early use of the account to build a profile of the customer to help spot potential account takeovers, remote attacks, and other fraud signals.

Voice Biometric Verification: Leveraging voice authentication by incorporating AI audio feature engineering. Some third-party tools offer functionality such as voice pattern recognition to reduce false positive identity authentication; this feature can be an effective complement to other traditional fraud signals.

Customer Profile Modeling: Developing AI/ML models and advanced analytics with data collected at onboarding to build a comprehensive customer risk profile to leverage during origination detection, transaction detection, and client-servicing.

Selfie Information: Many issuers have begun to request real-time applicant submitted selfies for potential high-risk account openings; this allows for facial recognition matching with photo IDs as well as the collection of metadata for customer profile analysis/modeling.

Advanced Fraud Detection Strategies:

Leveraging detection systems and strategies which centralize and analyze comprehensive data signals across all customer touch points and activities that integrate the data into real-time detection strategies and AI/ML risk modeling.

Targeted Alert Strategies: Because transaction detection for fraud app, ATO, and scams will result in alerts being sent directly to the responsible party, strategies like leveraging one-way alerts, push notifications, and exclusion-proof rules are key to stopping fraud/scam transaction from bypassing detection.

Transaction Behavior Strategies: Leveraging strategies that utilize past customer transaction behavior to detect anomalous high-velocity, high-dollar, or high-risk merchant spend. Scams and account takeover typically involve spend which is well outside the norm of the customer’s historic behavior, which offer fraud teams a reliable way to flag new high-risk activity and create targeted alerts to equip the front-line staff to service the customer appropriately.

Integration of Siloed Systems:

Integrating technology solutions that capture customer identity, behavioral, and transactional data across each stage of the customer lifecycle enables enhanced detection strategies and models to be leveraged throughout customer onboarding, anomaly detection, transaction detection, and customer servicing. Many institutions still rely on siloed detection systems that do not provide interoperability and the easy transfer of data, which can create system gaps that fraudsters aim to exploit.

Consumer Awareness:

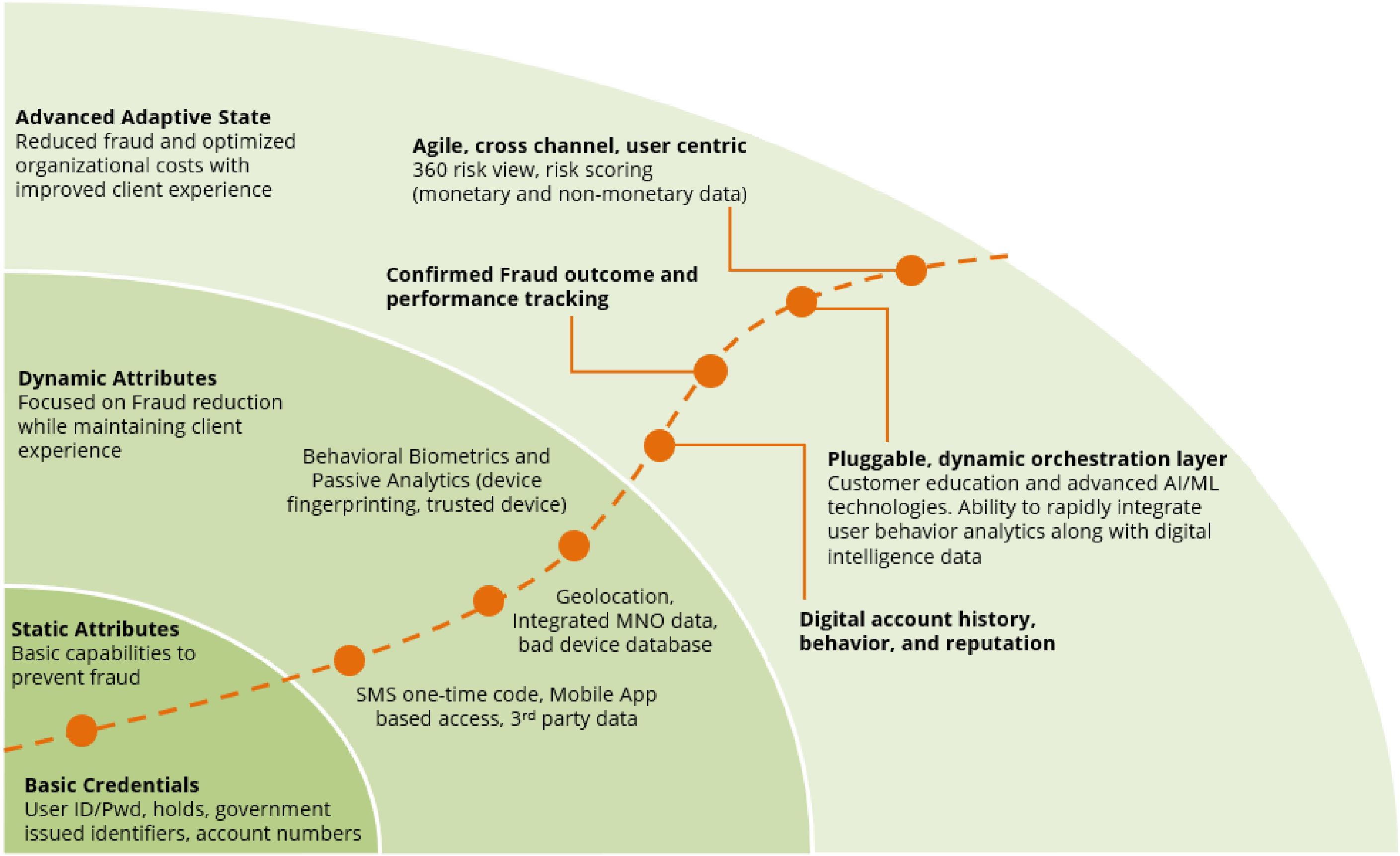
Investing in customer education can help to increase risk awareness related to payment services. Leveraging scam and fraud educatory content through online banking, email, direct mail, push notifications and in-branch/phone contact can enable customers to spot suspicious signs of fraud and be alert when transferring money or making purchases for third parties.

Front-line Staff Awareness:

Educating and training customer-facing staff is crucial to detect suspicious online customer interactions and transaction behavior. Front-line staff can educate customers who are unknowingly defrauded and contact the bank to push through high-risk transactions.

Figure 3. P2P Fraud Detection Evolution

Graphical depiction of the detection maturity journey that FI's undertake to enhance their capabilities from traditional static attribute detection to advanced adaptive tools and indicators.


Advanced Adaptive State
Reduced fraud and optimized organizational costs with improved client experience
Agile, cross channel, user centric
360 risk view, risk scoring (monetary and non-monetary data)
Confirmed Fraud outcome and performance tracking
Dynamic Attributes
Focused on Fraud reduction while maintaining client experience
Behavioral Biometrics and Passive Analytics (device fingerprinting, trusted device)
Pluggable, dynamic orchestration layer
Customer education and advanced AI/ML technologies. Ability to rapidly integrate user behavior analytics along with digital intelligence data
Geolocation, Integrated MNO data, bad device database
Digital account history, behavior, and reputation
Static Attributes
Basic capabilities to prevent fraud
SMS one-time code, Mobile App based access, 3rd party data
Basic Credentials
User ID/Pwd, holds, government issued identifiers, account numbers

Putting it All Together

Fraud mitigation in P2P has significant implications for financial institutions from customer education to usage of advanced analytics. There needs to be an integrated approach to managing the real-time detection, both on the customer level and the transaction level. With the recent momentum in the P2P space, there is a proliferation of players, fraud vectors, and various technological solutions in this space. Financial institutions are learning of ways to engage customers more effectively while integrating online fraud detection, identity proofing, and authentication. An end-to-end fraud management strategy will require focus on core capabilities like customer onboarding, monitoring integrity of the transaction process, and augmenting identity proofing processes to mitigate fraud. There is an increasing number of vendors in the online Fraud Detection space that offer integration across the entire customer lifecycle and provide key data points to enhance modeling and anomaly detection. Well-orchestrated fraud mitigation strategies need to leverage well-defined risk thresholds and policies, discern risk signals from multiple channels/sources, incorporate dynamic technological solutions throughout the customer journey, and provide robust consumer education. By moving strategically, financial institutions can build momentum on these core strengths to safeguard consumer trust and combat P2P fraud.

Let’s Talk

Deloitte Risk & Financial Advisory offers a wide range of strategy optimization, system integration, and model validation services to assist fraud teams with adapting to the changing fraud landscape and enhancing their detection capabilities. Through our breadth of cross-industry experience with financial service providers, Deloitte has developed an effective fraud risk management framework which considers benchmarks across end-to-end fraud operations, including people, process, technology, and security components.

End-to-End Fraud System Integration

Our team of specialists can assist with migration of legacy detection strategies, data sources, and detection models into new vendor solutions, as well as assisting in the development of new strategies to mitigate key pain-points and emerging fraud trends. We leverage our extensive cross-industry and cross-platform experience to help clients get the most value out of cutting-edge detection system functionality, analytical tools, and AI/ML detection models.

Detection Strategy Optimization:

Through our industry engagements and fraud specialists, we have a wide range of experience in identifying gaps, leveraging advanced analytical approaches, and using of industry-leading technologies to assist financial institutions in developing the optimal strategy framework for their specific loss challenges.

Model Development & Validation:

Deloitte Risk & Financial Advisory is experienced in validating proprietary and vendor-managed fraud models in line with regulatory guidelines and leading industry practices. Our specialists assist clients with a full lifecycle of model risk management services and related activities, including model development, governance, policies and controls, validation, and risk technology.

Operational Enhancement:

Deloitte Risk & Financial Advisory has assisted numerous clients across the financial industry with enhancing operational workflows, implementing advanced operational efficiency and impact analytics, and improving customer servicing and outreach. Our team of fraud specialists can help you get the most value out of customer servicing channels as well maximizing the efficacy and impact of customer communications for new product offerings, functionalities, and fraud and scam risks.

Trustworthy AI™:

Deloitte Risk & Financial Advisory uses a multidimensional AI framework to help organizations develop ethical safeguards across six key dimensions—a crucial step in managing the risks and capitalizing on the returns associated with artificial intelligence. Trustworthy AI requires governance and regulatory compliance throughout the AI lifecycle from ideation to design, development, deployment, and machine learning operations (MLOps) anchored on six dimensions in our Trustworthy AI framework.

Contacts

Damian Kuczma
Managing Director *| Deloitte & Touche LLP*
dkuczma@deloitte.com

Satish Lalchand
Principal *| Deloitte Transactions and Business Analytics LLP*
slalchand@deloitte.com

Devlina Lahiri
Senior Manager *| Deloitte & Touche LLP*
devlahiri@deloitte.com

Don Williams
Senior Manager *| Deloitte Transactions and Business Analytics LLP*
dowilliams@deloitte.com

Brendan Maggiore
Senior Manager *| Deloitte Transactions and Business Analytics LLP*
dowilliams@deloitte.com

Andrew Myers
Manager *| Deloitte & Touche LLP*
andmyers@deloitte.com

Lin Vuong
Analyst *| Deloitte & Touche LLP*
livuong@deloitte.com

Endnotes:

[1] Federal Trade Commission. "Fraud Reports." Public.tableau.com. Accessed December 20, 2022. https://public.tableau.com/app/profile/federal.trade.commission.12 and 13

[2] "Prime Time for Real-Time 2022." ACI Worldwide - GLOBAL PAYMENT TRENDS - Charting the growth of 'immediate payments'. Accessed October 25, 2022.

[3] "New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021." Federal Trade Commission, February 22, 2022. https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

[4] Consumers Union. "Peer-to-Peer Payments Are Generally Safe, but Consumers Must Be Aware of Risks." Consumer Reports, August 6, 2018.

[5] Jones, Huw. "UK Banks Told to Reimburse Customers Tricked by Scams." Reuters. Thomson Reuters, September 29, 2022.

[6] News, Joshua Roberts/Bloomberg. "WSJ News Exclusive | CFPB to Push Banks to Cover More Payment-Services Scams." The Wall Street Journal. Dow Jones; Company, July 19, 2022.

[7] "Consumer Response Annual Report January 1 – December 31, 2021." Consumer Financial Protection Bureau, March 2022. https://www.consumerfinance.gov/data-research/research-reports/2021-consumer-response-annual-report/.

[8] Tunggal, Abi Tyas. "The 68 Biggest Data Breaches (Updated for November 2022): Upguard." RSS, December 22, 12AD.

[9] Fletcher, Emma. "Reports Show Scammers Cashing in on Crypto Craze." Federal Trade Commission, August 11, 2022. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze#crypto1

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte Risk & Financial Advisory” means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.