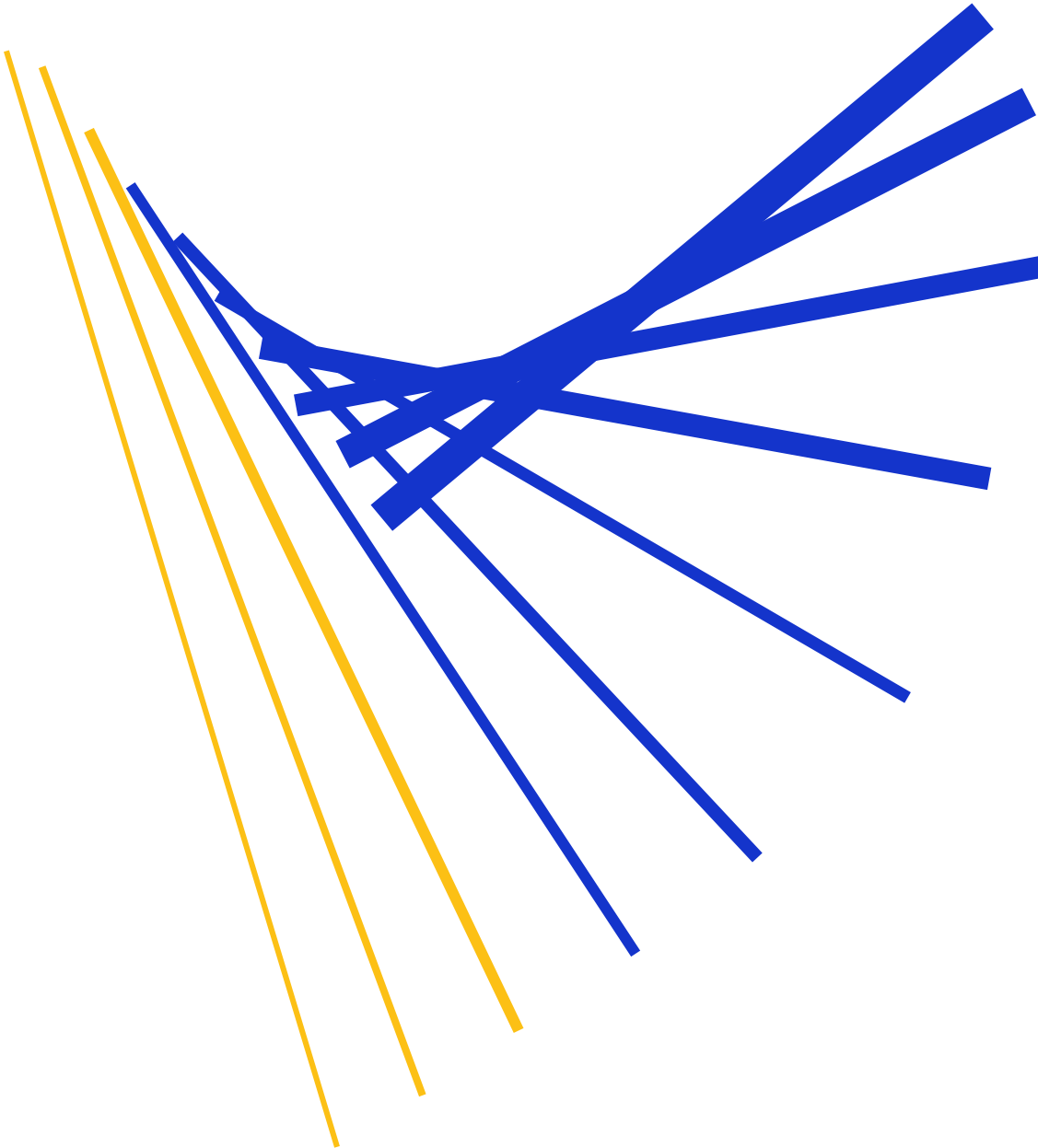


Best Practices for Issuers: Mitigating Crypto-Related Fraud

August 2022



Contents

- Context **3**
- Fraud Landscape **3**
- Fraud Mitigation Best Practices **5**
- Disputes **8**
- Conclusion **8**
- Annex A: Identifying Crypto Transactions **9**
- Annex B: Visa Fraud Tools.....**10**

ABOUT THIS GUIDE:

As a leader in payments, Visa remains focused on understanding risks inherent in the payment ecosystem.

This guide provides best practices for fraud prevention strategies and reminders of how to properly code crypto transactions to aid in the identification and risk assessment of these transactions.

Context

Visa has long served as a trusted engine of global commerce, enabling the secure and reliable movement of trillions of dollars between individuals, businesses, and governments in over 200 countries and territories. We believe that digital currencies will have a lasting impact on the future of financial services and money movement and as such, continue to pursue understanding risks inherent in the digital currency ecosystem.

Consumers continue to have interest in the purchase and sale of digital currency, including traditional cryptocurrencies (e.g., bitcoin), and stablecoins (e.g., USDC). **For the purpose of this document, cryptocurrency and stablecoins as well as CBDCs are collectively referred to as crypto.**

As consumer interest in crypto has grown, interest from threat actors has also increased. Visa regularly conducts analyses of issuer-reported fraudulent transactions and finds that most fraud reports related to crypto consist of account take over (ATO), unauthorized account use, or counterfeit or compromised payment account details. These fraud types are similar to fraud found in eCommerce/card not present (CNP) payment flows. Additionally, scams leveraging social engineering and first party fraud are also a concern.

This guide provides information relating to fraud monetization, mitigation strategies/tools and methods to identify crypto transactions that can be used in risk-based decisioning.

Fraud Landscape

Crypto is a new vehicle by which to engage in fraud activities due to several factors, including:

- Increased acceptance and use of payment accounts at crypto exchanges and by digital wallet applications that allow for the subsequent purchase of crypto
- Relative ease of the transaction process of crypto exchanges relative to other monetization methods, such as the physical nature and additional PIN data needed for ATM cash-outs, or the time and effort involved in monetization via the purchase and resale of digital or physical goods
- Speed at which money can be moved from the fiat ecosystem to the blockchain ecosystem, and the subsequent speed and ease at which crypto can then be moved to another, or multiple, addresses across the blockchain or moved to other blockchains
- Relative anonymity of blockchain transactions once money is moved to crypto ecosystems due to the difficulty of connecting the consumer's true identity to the wallet address





In addition, threat actors frequently use cybercrime underground forums to share tactics and tutorials on how to commit fraud and discuss monetization of stolen PANs via crypto on these channels. These forums are used to obtain the personal information needed to pass extra identification verification measures, including using open-source public records research websites and creating counterfeit documents and IDs.

Other topics of interest related to monetization via crypto include, but are not limited to:

- Step-by-step tutorials for monetizing stolen card data to crypto digital wallets
- Sale of user accounts and/or PANs with attached pre-verified (e.g., higher transaction limit) crypto exchange wallets
- Advice on which crypto to purchase and blockchains to use that allow for greater anonymity
- Identification of crypto exchanges, digital wallet applications, and peer-to-peer (P2P) services to use for greater monetization success
- Technical methods suggested for bypassing or overcoming fraud controls
- Use of third-party services to assist with government ID verification, fake name generation, phone number verification, and disposable email account creation

Common Fraud Monetization Methodologies

While threat actor interest in crypto as a monetization technique has grown, fraud methodologies linked to payment credential compromise are largely the same as CNP payment flows (e.g., enumeration, account takeover). The following table outlines the common fraud monetization methodologies.

Fraud Monetization Methodology	Description	Used in Direct Purchase of Crypto	Used in Wallet Funding Prior to Purchase of Crypto
Direct Crypto Exchange Purchase	Purchasing crypto directly from an exchange using a compromised PAN		
Cash-out Network	Used to establish multiple new accounts at exchanges with accounts used for cashing out funds via a mule network. Witting and/or unwitting participants are instructed to use stolen or enumerated payment accounts to purchase cryptocurrency via newly created exchange accounts. Once crypto is purchased and the account address at the exchange is funded, network members transfer the funds to a fraudster-controlled digital wallet address		
Peer-to-Peer (P2P) Mobile Application/Digital Wallet Application	Numerous P2P money transfer applications offer the capability to purchase, hold, and sell crypto. Using fraudulently obtained payment account details, individuals can initiate P2P money transfers to digital wallet accounts hosted on supported mobile applications. Once stolen funds are added to an account via a P2P transfer, fraudsters can subsequently purchase crypto		

Scams

One area of growing concern related to crypto is its use in scams, which occur when consumers are persuaded to undertake or support a fraudulent transaction using deception or manipulation. A scam can refer to any process or action that tries to successfully build trust (pseudo-trust) for a consumer to part with personal funds or data. Below are common social engineering methods used to perpetuate scams.

- **Email phishing/spear-phishing:** Email appearing to be from a trusted organization (e.g., popular brand or bank requesting victim to click on a link or to reply with PII). Spear-phishing messages specifically target and address the victim; purportedly coming from a trusted entity and containing personal information
- **Phone-based phishing (vishing/voice phishing):** Actors contact victims through phone calls requesting PII, card numbers, CVV2 codes, or OTP during the call
- **Text message phishing (smishing):** Exploits SMS or text messages sent to victims that typically contain links to phishing webpages, email addresses or phone numbers that when clicked may automatically open a browser window, email message, or dial a number
- **Website phishing/Malicious Advertisements or “Malvertizing”:** Leverages the greed factor (“too good to be true”) where illegitimate advertisements, sometimes involving local celebrities or reputed individuals without consent, promise high investment returns simply to obtain PII or card data.
- **SIM swap:** Type of account takeover scam, when attacker contacts a mobile provider and tricks the telco's staff into changing a victim's phone number to an attacker-controlled SIM card, enabling attacker to reset passwords and gain access to PII, email service, financial account information, or crypto trading systems

First Party Fraud

First party fraud (also known as friendly fraud, family fraud, buyer’s remorse, and accidental purchase) is a concern across the payment ecosystem and has become more prevalent with the growth of eCommerce and lack of customer friction in the dispute process. This occurs when a genuine transaction is claimed to be fraudulent by the customer who authorized it. This type of fraud has been historically difficult to quantify and requires the ability to prove the transaction was legitimately initiated by the customer and not by a fraudulent third party. Given the recent volatility in the overall crypto market, there has been a growing concern among issuers that volatility could cause buyer’s remorse and increase disputes related to first party fraud.

Fraud Mitigation Best Practices

Given threat actors are monetizing compromised payment credentials in similar ways as other CNP methods, existing CNP fraud mitigation strategies, techniques and tools can similarly be leveraged to mitigate crypto fraud. Issuers should consider their unique business model as well as risk appetite when developing a fraud mitigation strategy. Areas to include as part of a strong fraud mitigation plan include

- 1) Leveraging tools and strategies currently used for CNP transactions such as:
 - Predictive risk scoring tools, such as Visa Advance Authorization (VAA) or similar tool
 - A robust real-time rules engine to stop authorizations on the highest risk transactions, such as Visa Risk Manager (VRM) or similar tool

- A customer authentication strategy for incoming 3DS transactions, such as Visa Consumer Authentication Strategy (VCAS) or similar tool
 - A token provisioning strategy
 - Leveraging authentication data in authorization (e.g., data in Field 34 of the authorization message)
- 2) Reviewing and Monitoring:
- High volume or velocity transactions, or a combination of both, on a single PAN
 - Numerous declined attempts at a single crypto merchant or excessive declines at various crypto merchants
 - Suspicious monetization techniques, such as individuals conducting multiple purchases of crypto until an account is emptied
- 3) Reviewing accounts that were previously inactive, newly established, or have no history of crypto purchases that suddenly begin to transact at crypto merchants in high volumes and amounts
- 4) Instituting effective know-your-customer (KYC) measures to ensure that initial registrations of payment accounts are sufficiently reviewed and ensure the payment account device (if a virtual card) is associated with the known cardholder.
- 5) Enabling the Special Condition Indicator Code in field 60.4 of the authorization message, which contains the cryptocurrency indicator (value of "7"), as it can be used in risk-based authorization decisioning

Scam Mitigation

The best offense in preventing scam fraud is providing education and awareness to cardholders and employees about phishing, smishing, and vishing campaigns. Consumer education and empowerment are important to prevent social engineering (e.g., how to identify red flags). In addition, issuers should:

- Develop strong up-front identification and verification procedures. Ask less commonly used questions or questions regarding other accounts the customer may have or transactions they may have made
- Use third-party tools to assess the risk of consumer session data elements (e.g., email, IP address, phone number, device fingerprint) and monitor consumer session data elements to identify atypical access patterns
- Consider limiting the number of PANs that can be provisioned to a single mobile device
- Require multi-factor authentication (MFA) when provisioning a PAN to a mobile device and use secure OTP delivery methods such as dedicated OTP applications
- Monitor high-risk account changes and logins, coupled with high-risk transaction or authentication activity.
- Monitor a cardholder's online banking sign in activity to identify credential stuffing or abuse.
- Include additional information with transaction alerts and authentication messages that empower cardholders to detect illegal activity with their accounts (e.g., 3DSecure or remote banking OTPs can contain notice that the password will be used to perform a financial transaction or provisioning a card to a mobile device or digital wallet).

- When using 3DS, ensure that the merchant’s name matches in authentication with authorization to detect abnormal activity making it easier for cardholders and issuers to recognize transactions. In case of a mismatch, risk evaluation of the transaction is recommended to prevent fraud.
- Use SIM swap data during online transactions or authentication process provided by Mobile Network Operators across many geographies¹.
- Peer-to-Peer (P2P) payments –sending and recipient issuers should consider implementing manual or automated transaction monitoring mechanisms or implement models to detect anomalous activity as part of their risk management program.
- Monitor call centers for spikes in calls from account holders regarding unauthorized changes to their accounts.

To support the changing fraud landscape, effective October 2021, two new fraud types, **Fraud Type C** and **Fraud Type D**, were introduced as outlined below.

- **Fraud Type C (Merchant Misrepresentation):** Fraud resulting from a merchant deliberately misleading the account holder. Examples may include a merchant fraudulently selling items that are not as they seem or are sub-standard, charging more than anticipated or for a longer term, or charging for a service that the consumer can get for free through another channel.
- **Fraud Type D (Manipulation of Account Holder):** Fraud resulting from a merchant manipulating an account holder into completing what they believe to be a legitimate transaction. This fraud type was added to support Visa Direct and the European Payment Services Directive 2 (PSD2) regulations. Examples may include account holders manipulated into sending funds to a fraudulent beneficiary when the sender believes they will gain fictitious riches or help an individual in distress or a struggling business, or to pay medical fees - and/or - a bad actor contacting the sender to impersonate a known supplier, trusted organization, or business to request a change of payment details for a transaction or to request a payment to a fraudulent account.

In addition, the current rules for **Dispute Category 10—Fraud** prohibit an issuer from processing a dispute on a transaction that was approved using a payment credential for which the issuer had reported fraud activity. This rule is designed to encourage issuers to close the payment credential to prevent future fraudulent usage. However, because **Fraud Types C and D** encompass scenarios in which the cardholder has participated, the issuer is not required to reissue the payment credential and retains the right to process a dispute on future fraudulent transactions.

First Party Fraud Mitigation

Closely monitoring activity for any cardholder who appears to be a serial disputer and deploying mitigation strategies, as outlined below, is critical to reducing first party fraud. To mitigate first party fraud, Issuers should:

- Establish reasonable thresholds to determine a pattern of bad cardholder behavior

¹ "What You Need to Know about Sim Swap Scams: AT&T Cyber Aware." *AT&T News, Wireless and Network Information*, 14 Sept. 2017, https://about.att.com/pages/cyberaware/ni/blog/sim_swap.

- Incorporate controls that establish reasonableness of cardholder claim and de-incentivize cardholders from committing this type of fraud
- Determine if the cardholder has previous/post transactions to the same merchant and present evidence to customer for review
- Perform a formal review of the customer's account(s) if the customer has had multiple fraud claims, regardless of merchant
- Consume and leverage near real time disputes system data like **Order Insight**, a service offered by **Verifi**, a **Visa solution**, which connects issuers with a global network of merchants to share transaction details with the issuer and cardholder to resolve disputes in near real time and prevent costly chargebacks

Disputes

Disputes for crypto purchases should be handled in the same manner as all other disputes. There are no separate dispute conditions for crypto. All disputes must comply with applicable rules in Section 11 Dispute Resolution of the Visa Core Rules and Product and Services Rules. Dispute rights are based on the nature of the claim and the processing codes which are used in the transaction.

Account Funding Transactions

For transactions processed as an account funding transaction (Processing Code 10), issuers may have dispute rights under Condition 13.1 (Merchandise/Services Not Received) if the funds were not transferred to the consumer's account.

Purchase of Crypto

For transactions processed as a quasi-cash transaction (Processing Code 11), issuers may have dispute rights under Condition 13.1 (Merchandise/Services Not Received) if the crypto was not received. The service is deemed as received once crypto is deposited/credited into the consumer's wallet/account.

Please note: *In response to the dispute, the acquirer must provide evidence that crypto was deposited/credited into the consumer's wallet/account.*

Conclusion

As consumers continue to engage in the purchase crypto, it's important for issuers to maintain strong risk management practices. There are varying degrees of fraud methodologies and monetization techniques bad actors can use in the crypto ecosystem. Visa has provided this best practice guide as one way of supporting issuers' risk-based decisioning processes, fraud reduction, and fraud prevention strategies when enabling the purchase of crypto. As a leader in payments, Visa remains focused on understanding risks inherent in the payment ecosystem.

For questions, please contact your Visa representative or visit Visa Online for access to additional materials.

Annex A: Identifying Crypto Transactions

To enable Issuers to identify and evaluate crypto transactions in risk-based decisioning, Visa requires a Special Condition Indicator. Special Condition Indicator with a value of "7" in field 60.4 of the authorization message identifies crypto purchases. Issuers should ensure field 60.4 is enabled as this allows the indicator to be used as part of the identification and evaluation of each transaction in risk-based decisioning when authorizing crypto transactions. Documentation regarding this field is located in the Visa technical specifications documentation which is available at Visa Online (VOL). The table below outlines various transaction scenarios, effective April 23, 2022.

Scenario	Merchant Category Code	Processing code	Business Application Identifier (BAI)	Crypto Indicator (7) in Special Condition Code Field?
The consumer is acquiring cryptocurrency in a transaction.	MCC 6051 - Non-financial institution MCC 6012 - Financial institution	Quasi-cash (QC) indicator ² (Processing code 11)	N/A	Yes
The consumer is loading a cryptocurrency wallet or exchange account with fiat.	MCC 6051 - Non-financial institution MCC 6012 - Financial institution	Account funding transaction (AFT) indicator (Processing code 10)	Funds Transfer (FT) Wallet Transfer (WT)	Yes
The consumer is loading a general purpose wallet with many uses (e.g., investing, prepaid balance, cryptocurrency) with fiat from a non-credit card.	MCC 4829 - wallet whose primary business is wire transfer / P2P money transfer MCC 6012 – wallet that is a financial institution MCC 6540 - general purpose wallet that is not a financial institution	AFT indicator (Processing code 10)	Funds Transfer (FT)	No
The consumer initiates a disbursement of converted fiat from FI-licensed entity (bank, credit union, or wallet) or FINRA-licensed ³ (brokerage) to a bank account via PAN.	MCC 6211 – FINRA-licensed brokerage MCC 6012 – Other FI-licensed entity	Original Credit Transaction (OCT) indicator (Processing code 26)	Account to Account (AA)	Yes
The consumer initiates a disbursement from a crypto-capable brokerage/wallet to a Visa card.	MCC 6051 – crypto wallet or exchange MCC 6211 – brokerage MCC 4829 – general purpose wallet	Original Credit Transaction (OCT) indicator (Processing code 26)	Funds Transfer (FT) Wallet Transfer (WT)	Yes

² If the transaction is a domestic transaction in the US, an AFT can be used until April 2025

³ US only

Annex B: Visa Fraud Tools

Various fraud tools are available to Visa clients which can be leveraged to mitigate crypto fraud.

Tool name	Short Description
Visa Advanced Authorization (VAA)	<p>Powered by artificial intelligence and Visa’s global data, VAA analyzes the network for emerging fraud patterns and identifies transactions that do not fit individual usage patterns to deliver a real-time risk score to help predict the likelihood of fraud.</p> <ul style="list-style-type: none"> • Evaluates up to 500 unique risk attributes per transaction providing global issuers with sophisticated in-flight transaction risk scoring, for more targeted and better-informed authorization decisions. • Delivers a two-digit risk ranging from 1 (low risk) to 99 (high risk). • Data collection rides on Visa Net processing; no capital investment or additional data is required. • Allows issuers to manage high and low risk activity. • Frequent data updates allow for a faster reaction to emerging fraud trends.
Visa Rules Manager (VRM)	<p>VRM is a web-based suite of tools designed to provide issuers with control and flexibility to manage fraud risk and optimize authorizations. VRM allows issuers to write rules with more than 70 transaction parameters (including the VAA score) and test those rules before publishing them to enable real-time decisioning of transactions. Flagged or declined transactions can also be added to a case management queue to validate fraud or false declines.</p> <ul style="list-style-type: none"> • Issuers have more control and flexibility to manage their risk strategies based on their own risk tolerance. • Create, test, and publish custom strategies using a web-based interface in minutes.
Visa Token Service (VTS)	<p>Visa Token Service (VTS) replaces the consumer’s primary account numbers (PAN) with a unique digital identifier (a “token”) that can be used for payment without exposing a cardholder’s PAN. The resulting transactions are secured with unique transaction-based data (cryptogram), making consumers’ data more secure and further reducing fraud risk if the token were to be compromised. Tokens can support new payment experiences as merchants, issuers and digital partners can use tokens to create a seamless omnichannel payment experience.</p> <ul style="list-style-type: none"> • More secure transactions – Every consumer-initiated transaction with a Visa token requires a unique cryptogram, effectively securing stored payment information at rest, and protecting against fraudulent replay of payment data in transit. • Preserve ‘top-of-wallet’ status - When issuers provide PAN updates to VTS, a cardholder can continue transacting with the provisioned token even when the underlying card information changes. This can lead to higher approval rates and better consumer experiences, as the cardholder will not be prompted to replace their card with an alternative payment method due to expired credentials. • Reducing card re-issuance costs - If a token is compromised (e.g., a mobile phone is lost or stolen), the token can be suspended or deleted without needing to reissue the physical card.

Tool name	Short Description
Visa Consumer Authentication Service (VCAS)	<p>Visa Consumer Authentication Service (VCAS) is a data-driven, hosted solution designed to support an issuer’s authentication strategies within their 3-D Secure program. At the core of the product is its risk-based authentication capabilities, which help to reduce friction during checkout, while providing a higher level of security. It works behind the scenes to evaluate each transaction based on an exchange of data between the merchant, issuer, and Visa. VCAS provides issuers with risk-based authentication using Visa’s proprietary risk score. This solution assesses the risk of a transaction in real-time using predictive risk analysis based on enhanced inputs, including device and transaction information and behaviors. This network-wide level of intelligence gives issuers the ability to decide if and when additional authentication is needed. The VCAS risk model uses hundreds of data points to score a transaction, which can be broadly grouped into account/transaction, and device related data. Account data includes account transaction history, confirmed fraud and chargebacks, merchant profiles, and compromise event-related information. This data set includes Visa’s network-wide view of the transaction – across all Visa issuers, acquirers, and merchants. Account/transaction data coupled with device information such as device ID, IP address, session information, operating system, geographic location, etc., result in a powerful VCAS risk score ranging from 01 to 99; the higher the score, the higher the risk; the lower the score, the lower the risk.</p>
Order Insight	<p>Order Insight provides issuers and cardholders access to enhanced seller and purchase details from sellers to prevent disputes at the point of first customer inquiry, helping avoid unnecessary disputes from being processed. Order Insight is implemented in Visa Resolve Online (VROL) and connects issuers with sellers on a global scale. Order Insight enables issuers to validate sales, improve the cardholder experience, identify true fraud, and prevent friendly fraud. Order Insight is also available for non-Visa portfolios for enhancing the cardholder engagement and/or back-office dispute processing.</p> <p>Order Insight Digital provides the same enhanced merchant and purchase details to cardholders directly through the issuer’s mobile or desktop banking applications for both Visa and non-Visa transactions. Providing this data directly through the digital channel empowers the cardholder to achieve self-resolution, negating the cardholder’s need to call an issuer call center. Order Insight Digital improves the customer experience and extends the seller’s customer service.</p>
Account Name Inquiry (ANI)	<p>Account Name Inquiry (ANI) offers merchants and acquirers the ability to conduct a verification of account name information prior to authorization or full financial requests. The solution assists in fraud mitigation against unauthorized card use, account takeover and authorized push payment/Scam fraud.</p> <p>US AFT/OCT Pilot opportunities are available. If interested contact your Account Executive.</p>