VISA

Instant Digital Issuance: Best Practices on Fraud Management

Protecting the future of payments

Table of Contents

Instant Digital Issuance

Summary

The future of payment cards is an all-digital end-to-end payment experience. Instant digital issuance (IDI) offers real-time account creation and delivery of a ready-to-use credential to a cardholder through a digital channel. It's a critical first step to a fully digital experience, delivering on-demand creation and provisioning of digital payment credentials that can be used for face-to-face Point of Sale (POS) and e-commerce purchases, alike.

As more and more issuers are opting for IDI as a way of issuing cards, it is imperative for financial institutions to understand potential risks associated with going fully digital and become informed on various best practices discussed in this white paper as a way to mitigate those risks and create a safe and meaningful experience for the customer as well as for the issuers.

In this paper, we will discuss IDI in detail, the growth drivers and benefits of IDI, and share the best steps you can take to mitigate related fraud.

Problem Statement:

Approved! Your card will arrive in 5 to 10 business days.

Instant Digital Issuance Overview

Where we go from here

Demand for IDI continues to grow with the shift to digital commerce and enhanced consumer experience. This is further accelerated by the pandemic.

Today, only **10%** of U.S. financial in titutions (FIs) offer IDI and push provisioning; however, this number is expected to grow to over **50%** by 2024[1].

The benefits of IDI

Enhanced Customer Experience

IDI eliminates the hassle of receiving the card by mail or collecting from the branch, ensuring 100% delivery of the digital card credentials

Increased Revenue

Quicker activation and higher usage rates mean increased business

Improved Customer Retention

Drive better business outcomes with IDI

[1] In-Branch Instant Issuance – Cardholder Benefits and Competiti e Advantage, Aite Novaricia, November 2021

Use cases

Common global use cases include new customer acquisition strategies via the issuer or issuer partners, existing customer optimization strategies like lifecycle management and up/cross-selling products, and additional utility use cases.

Scale to distribution

Remote application and remote issuance streamline the process and cut down the additional leg of visiting the branch or meeting an executive to collect the required Know Your Customer (KYC) and credit risk evaluation documents. This presents scale to distribution and makes it a 24x7 available channel to have the card issued, activated immediately, and used thereafter.

Enablement

The issuer processor is typically the core enabler of IDI functionality.

- The capabilities of the issuer processor, in conjunction with the issuer's capabilities, determine the ease or complexity of the move to IDI.
- Potential challenges include limitations of bank legacy systems, lack of real-time account creation capabilities, and other technology constraints. When it comes to new to bank customers, instant KYC verification capability is a key dependency.
- The initial steps to enable IDI for payment portfolios include consultation with the issuer processor, technology enablement, fraud risk assessment and mitigants, customer journey design, and business case formulation. Visa services, partnerships, and products can help resolve gaps identified in the initial analysis.

Digital Issuance vs. Instant Digital Issuance

	Traditional	**Instant**
Physical	Traditional Issuance Creating and delivering a physical payment card that will be ready for use after physical card activation (5-10 business days) *Ex. Plastic card delivered by mail*	Instant Issuance Creating and delivering physical payment cards instantly that are ready for use in real-time *Ex. Plastic card printed in branch*
Digital	Traditional Digital Issuance Creating and delivering payment credentials that are accessed through a digital user interface and ready for use after physical card activation (5-10 business days) *Ex. Existing card manually provisioned to mobile wallets*	Instant Digital Issuance Creating and delivering payment credentials instantly that are accessed through a digital user interface and ready for use in real-time *Ex. Real-time approval, creation, issuance and provisioning to mobile wallets*

Growth Drivers & Benefit of Instant Digital Issuance

A look at what's propelling the adoption of IDI

Time Is Money

IDI can reduce the time between issuing the card and getting the card to the customer from 5-10 business days to 5-10 *minutes*.

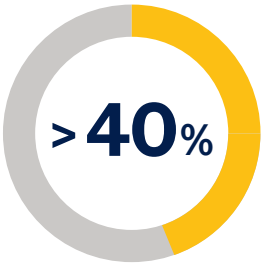
1. IDI can help obtain and maintain 'top-of-wallet' status

Up to **25%** of top-of-wallet status is lost each year*

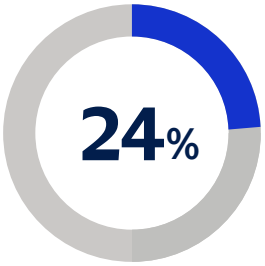
Given that top-of-wallet cardholder spend is up to **4X** of average spend level of the portfolio, this churn has significant implications.

Once a top-of-wallet position is relinquished, the risks of purchase inactivity are heightened. This, in around 40% of cases, leads directly to active attrition[1].

2. IDI attracts and engages digital-native customers



of retail bank customers who switched banks wanted to bank with a more innovative provider[2]



of banking customers globally said they would be less likely to visit a branch as a result of change in behavior due to the COVID-19 pandemic[3]

3. IDI leads to increased usage

+5 debit transactions per month for instant issued cards*

5% **increase** in overall transaction volume[4]

4. IDI leads to decreased customer servicing costs

- Lower customer support expenses with digital self service enhancements, allowing customers to solve more problems on their own
- Lower costs vs. in-branch physical card issuance with on-site machines and card stock management, including handling returns and destroying them

*Visa Analysis

[1] The importance of tracking customer engagement through the COVID-19 pandemic- VCA -Oct'20

[2] Global Data, Digital OnlyBanks: Threat or Motivator?, December 2018

[3] Retail Banking in the New Reality, Survey, Boston Consulting Group, May 2020

[4] Instant Issuance is Revolutionizing Financial Institutions' Customer Experience, Harland Clarke, 2018

Instant Digital Issuance Universal Flow

Understanding risk and staying informed

Instant issuance of digital card accounts involves the combination of several stages where sensitive information is exchanged between the consumer and their issuer. Besides securing the data, the information must be correct, authenticated, and secure since the issuer is relying on it to make decisions related to the consumer like credit line extension, for example, and eventually sharing the payment card credentials digitally.

Given the multiple risk considerations, mitigation strategies, and potential solutions to ensure the correctness and authenticity of the data, the objective of this document is to help issuers with the following:

a) Understand the potential fraud risks involved in IDI

b) Get informed on leading strategies to mitigate those fraud risks

Stages in Instant Digital Issuance Universal Flow

IDI can be de-constructed into the following four stages for better understanding ecosystem roles and industry benchmarks:

- **Origination**
- **Onboarding**
- **Activation**
- **Usage**

	Origination		Onboarding		Activation		Usage	
	Capture	**Processing**	**Account**	**Issuance**	**Activation**	**Delivery**	**Transact**	**Management**
Acquisition	Completely digital application data capture and ID verification	Risk and fraud checks (eKYC, AML, OFAC) and Credit decisioning	DDA or line of credit account approval and creation	Real-time credentials generation, Issuance and funding	Separate activations for physical card and digital PAN	Push provision digital credential to tokenized use cases (Wallets and COF)	Ready for face-to-face and digital card display for CNP transactions	Provide card controls and management tools
Reissuance	Completely digital lost & stolen request	Perform fraud checks and instant reissuance eligibility	Block card and update status (Fraud/No Fraud)	Real-time PAN generation and issuance	Separate activations for physical card and digital PAN	PAN lifecycle updates for token and non-token use cases	Ready for face-to-face and digital card displays for CNP transactions	Display COF merchant updates and manage subscriptions
Benchmark	**3 minutes** to take an application or lost/stolen request		**2 form factors** with digital PAN issued first and optional physical card to follow		**1-click activation and delivery** to digital channels		**Available everywhere** from over 100M+ merchant locations as of September 30, 2021[1], major wallets, e-commerce and card-on-file, and at contactless-enabled ATMs	

From 5-10 Business Days to 5-10 Minutes!

Visa helps clients achieve the Instant Digital Issuance target of **"3 –2 –1 –Everywhere"**

Key Terms:

AML - Anti-Money Laundering
OFAC - Office of Foreign Assets Control
DDA - Demand Deposit Account
COF - Card-On-File
CNP - Card Not Present
PAN - Primary Account Number

[1] Visa Fact Sheet

Best Practices on Fraud Management with Instant Digital Issuance

Four steps to mitigate fraud

Step 1: Origination

One of the risks at the origination step is incorrect/false information provided in the application. In order to mitigate the risk, the best practices below can be used to verify the identity of the applicant and validate the accuracy of the information.

Nation specific centralized database

Issuers can use the nation specific entralized database of user information. This will help issuers reduce credit and fraud losses and protect consumers from being affected by identify theft and other types of fraud. Issuers can make the facial image field as a manda ory input in the application while applying for IDI of the card. They can then use this image and run it against the nation specific entralized database of user information to verify the information provided by the applicant. To enable any of the checks in response to the application, a second factor of authentication will confirm the customer's request. Care needs to be exercised to exclude customers who have recently changed their mobile number or e-mail ID, for a reasonable period of time.

Issuers can also run additional behavioral analytics on mouse movement around screen, typing speed/speed to fill out fields, oing back pages or changing tabs during app process and many more.

Determine appropriate level of validation strictness on name and address verification (AVS)

Issuers must determine the level of validation strictness concerning name and address verifi ation (AVS) required for provisioning purposes and/or find a methodology f assisting cardholders in minimizing the variability of name and address data entry. As cardholders can enter address and name data in a multitude of different ways (i.e., punctuation, abbreviation), issuers need a methodology either to drive consistency in terms of data entry (e.g. leveraging official ad ess data from the postal service) and/or adjust the level of validation strictness.

Tracking of individual systems/devices

Issuers should continuously monitor the geographical location from where the applicant is applying for IDI of card via tracking the Internet Protocol (IP) address of the device. This can help identify a potentially fraudulent activity where a fraudster could be trying to open an account in a bank located outside of his own geographical location or if multiple accounts are being opened using the same device/system.

Separate card number ranges based on the type of issuance

Issuers can allocate different BIN ranges of 16-digit card numbers based on the type of issuance i.e., different BIN ranges for digital issuance and IDI. This would help issuers to apply different set of fraud rules for different types of issuance requests and thus enhance security.

Step 2: Onboarding

In this step, the account of the cardholder is created, credentials generated and (re)issued. Once the credentials are activated for the cardholder, it can become prone to enumeration attacks, i.e., use automation to rapidly iterate through numeric sequences to identify PAN and CVV2 combinations. The below suggested best practices can help reduce this risk:

Use of non-sequential PAN and dynamic CVV2

Issuers can use non-sequential PAN while generating the PAN for the cardholder. This will help mitigate the risk of enumeration attacks.

For all card not present transaction scenarios, issuers should choose to provide dynamic CVV2 (dCVV2) to the cardholders. This generates a new CVV2 each time an e-commerce transaction is initiated and can help mitigate the risk of enumeration attacks.

Deploy spend controls

One of the risks at this stage of IDI of card is approval and instant availability of full credit line or available balance, as the case may be. This may lead to misuse of funds in case of fraudulent activity.

- One best practice to mitigate the fraud activity is to set limits on the initial purchase amount. The issuer can increase the purchase limit upon establishing the authenticity of the cardholder. For example: In a digital first issuance process, after the cardholder has successfully authenticated via mobile app, or after receiving and activating the physical card.
- Another control can include setting separate spending limits on each form factor, such as the IDI credential vs. the physical card.
- Limiting transaction types and excluding high risk Merchant Category Code (MCC) for the digitally issued credential to allow expected card not present transactions can limit the risk of unauthorized transactions. Stepping up the card not present transactions and seeking a second level of authentication further protects the issuer.
- Setting specific controls on the types of card purchases and spending patterns can alleviate some risk of fraudulent activity. For example: An IDI credential can be assigned a separate set of fraud rules vs. the physical card (such as through the Risk Services Manager tool). This can include time-based risk assessments on authorizations. If not performing time-based risk assessments, the assigned fraud rules can be changed when the physical card is activated.

It is recommended to enable reporting and perform ongoing risk assessments for all digitally issued credentials.

Step 3: Activation

In this stage, activation and immediate provisioning of digital credentials to access banking application takes place.

A key decision to take is whether to use the same PAN for the instantly-issued digital credential as well as the physical card to follow, or go with a different PAN for each. Consider both advantages and disadvantages, below:

1. Two Different PANs

Advantages	Disadvantages
• Multiple PANs offer an isolated channel for transactions with a 16-digit number different from the physical card which arrives in a deactivated state. • More than enumeration attacks, it prevents physical card interception and the ensuing fraud. The enumeration attack possibility is not mitigated.	• Using multiple PANs can create confusion for the consumer in terms of knowing the right PAN number to use. • Consumer can face issues updating the information of the saved PAN details and with service providers in case of using multiple PANs or in case of re-issuance.

2. Single PAN

Advantages	Disadvantages
• Using a single PAN for transactions will avoid the confusion for the consumer compared to multiple PANs.	• The physical card arrives in the activated state for various types of channels. As a mitigant, you could follow the 'Channel-based Activation: Suggested Best Practices' table in page 12 of this white paper, below.

Once the account for the cardholder has been activated on the banking application, there is an opportunity to further establish the card as top of wallet by pushing the newly created account onto other payment applications and channels via a push provisioning process.

Push Provisioning

Instantly enable spend by pushing digital credentials into mobile wallets, card-on-file COF) merchants and Click to Pay.

Adding a credential to a digital wallet tokenizes the card. Card tokenization replaces the card number with a randomly generated number, known as a token. Using tokens ensures that card information cannot be compromised during the transaction and provides a more secure payment method than legacy methods.

Building in-app provisioning can be complex and expensive. Clients may have to make substantial investments to build out push provisioning capabilities, hastening time to market. In addition, considerations such as maintenance of wallet endpoints, wallet provider updates, compliance and regulatory requirements, etc. can further pose challenges to maintenance of in-house solution. However, clients can deploy provisioning solutions offered by partners that accelerate time to market while minimizing the upfront and ongoing investment.

Step 4: Usage

This is the final tage which includes cardholder transaction and account management. In this phase, a cardholder should be able to retrieve card details from their mobile banking app in order to conduct face-to-face contactless transactions, besides e-commerce transactions.

Here are some ways to enhance security while exposing card details:

1. Notify the cardholder of their new credential
2. Authenticate the cardholder before allowing card activation. This can include knowledge-based questions and answers, one-time passcode step-up, or other validation steps to confirm that the in ended card recipient is the correct cardholder.
3. Set a timer for the screen, which will return the user to the previous or home screen after a short period of inactivity
4. Disable the ability to take a screenshot when this data is presented to the user
5. Mask or blacken the screen if the user moves the mobile app to the background
6. Disable the ability to “cut and paste” the data for use with another application or prevent copying data to the device’s clipboard

Ensure a channel-based activation strategy

Visa recommends a channel-based activation strategy to mitigate transaction fraud risk. See the chart below for guidance:

	Magstripe	Contact Chip	Contactless Chip		E-commerce		ATM		Money Transfer Service
Data Fields	PEM 90 Transaction type 01 = Cash Withdraws Transaction type 30 = Available Funds Inquiries	PEM 05	PEM 07		PEM 01; ECI 5, 6, 7; AVS		MCC 6010/6011; Transaction type 01, 30		
			PAN	Token	PAN	Token	PAN	Token	
New Account Creation	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Push Provisioning of Pays / Banking App	Disabled	Disabled	Disabled	Enabled	Disabled	Enabled	Disabled	Enabled	Enabled
Display of PAN / CVV2 In App	Disabled	Disabled	Disabled	Disabled	Enabled	N/A	TBD	Disabled	Enabled
Display of Token / CVV2 In App	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	TBD	Enabled
Delivery of ATM PIN	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Disabled
Delivery of Physical Card	Enabled	Enabled	Enabled	N/A	Enabled	N/A	Enabled	N/A	Enabled

Tick Mark Legend	
N/A	Not Applicable - The corresponding channel-data field ombination is not feasible
TBD	To be decided based on client needs

Support the use of tokenization for secure and successful transactions

Tokenization replaces sensitive account information, such as a 16-digit account number, with a unique digital identifier called a token. Tokens allow payments to be processed without exposing actual account details that could potentially be compromised. Other benefits of tokenization include enablement of digital wallets, and improved authorization rates for online transactions.

Key Terms:

PEM - POS Entry Mode (POS - Point of Sale)
PEM 01 = Manual Key Entry
PEM 07 = Contactless
PEM 05 = Card on File
PEM 90 = Magnetic Strip
ECI - Electronic Commerce Indicator
Transaction type 01 = Cash Withdraws
Transaction type 30 = Available Funds Inquiries
AVS - Address Verifi ation Service
MCC - Merchant Category Code
MCC 6010 = Financial Institutions Manual Cash Disbursements
MCC 6011 = Financial Institutions, Automated Cash Disbursements
PAN - Primary Account Number
CCV2 - Card Verifi ation Value 2

How Visa Can Help

Visa has the necessary tools and services which can assist the issuers in implementing the below mentioned best practices for each stage in the IDI lifecycle:

Visa has the necessary tools and services to assist financial institutions in implementing IDI best practices along each stage of the IDI journey. For the origination stage, financial institutions can deploy Visa ICS, a risk management product used to bolster credit underwriting and fraud prevention.

Next, for onboarding, Visa provides APIs and tools such as Visa Account Updater Suite and for activation of the issued cards, Visa offers solutions such as Visa Token Service (VTS), Visa Card Enrollment Hub (VCEH), Visa In-App Provisioning (VIAP) API and SDK to further strengthen financial in titutions' internal fraud capabilities.

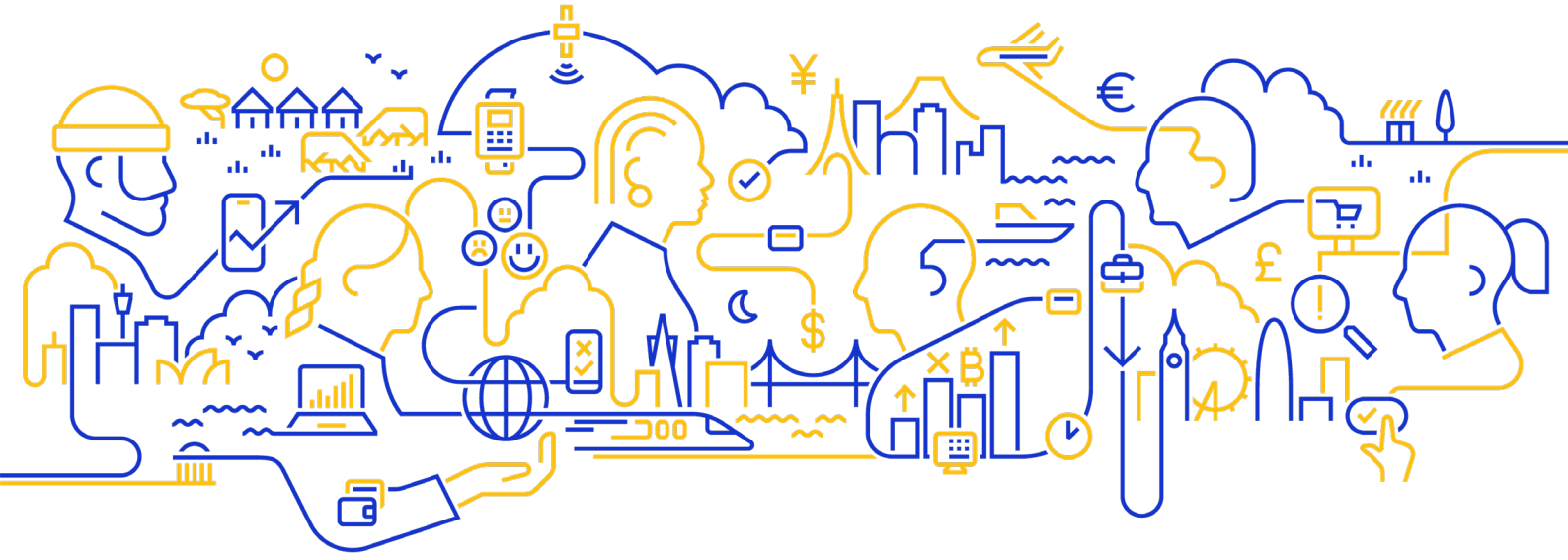
Lastly, when financial in titutions are ready for the usage stage, they can leverage multiple tools including Visa Risk Manager (VRM), Visa Transaction Controls (VTC) and Risk Services Manager (RSM), as well as Visa Consumer Authentication Service (VCAS) and Visa Advanced Authorization (VAA) to enhance scoring mechanisms and better detect, prevent and mitigate transaction fraud.

For more information on Visa products listed above, please speak to your Visa representative.

About Visa Consulting & Analytics

Visa Consulting & Analytics (VCA) is ideally positioned to work with clients to help formulate IDI business case/opportunity sizing, roll-out strategy, user journey design and fraud capabilities assessment, including recommendations to address gaps.

- Our consultants are experts in strategy, product, portfolio management, risk, digital and more with decades of experience in the payments industry.
- Our data scientists are experts in statistics, advanced analytics and machine learning with exclusive access to insights from VisaNet, one of the largest payment networks in the world.
- Our economists understand economic conditions impacting consumer spending and provide unique and timely insights into global spending trends. The combination of our deep payments consulting expertise, our economic intelligence and our breadth of data allows us to identify actionable insights and recommendations that drive better business decisions.



For more information, please contact your Visa Account Executive, email Visa Consulting & Analytics at **VCA@Visa.com** or visit us at **Visa.com/VCA**

Follow VCA on **LinkedIn**