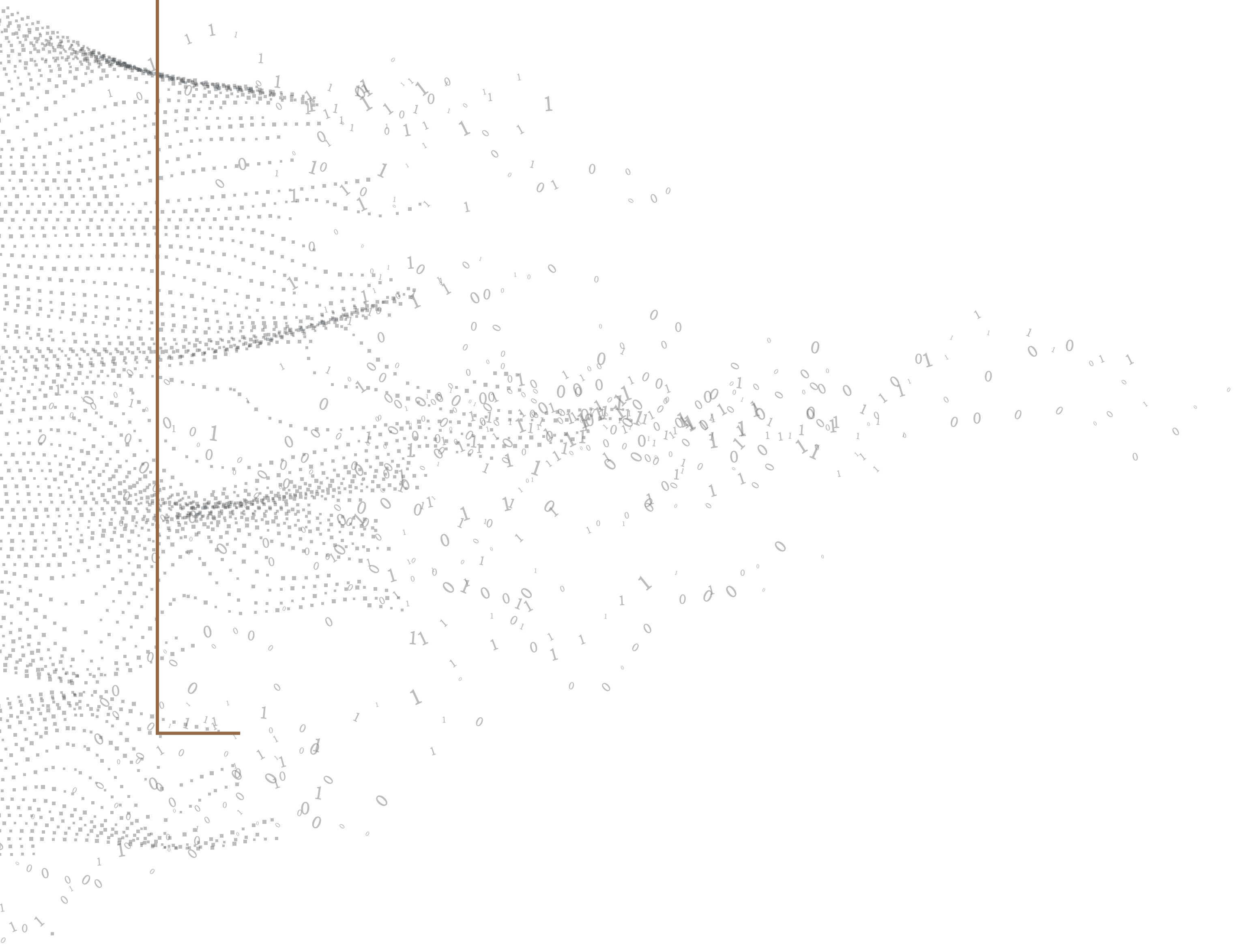
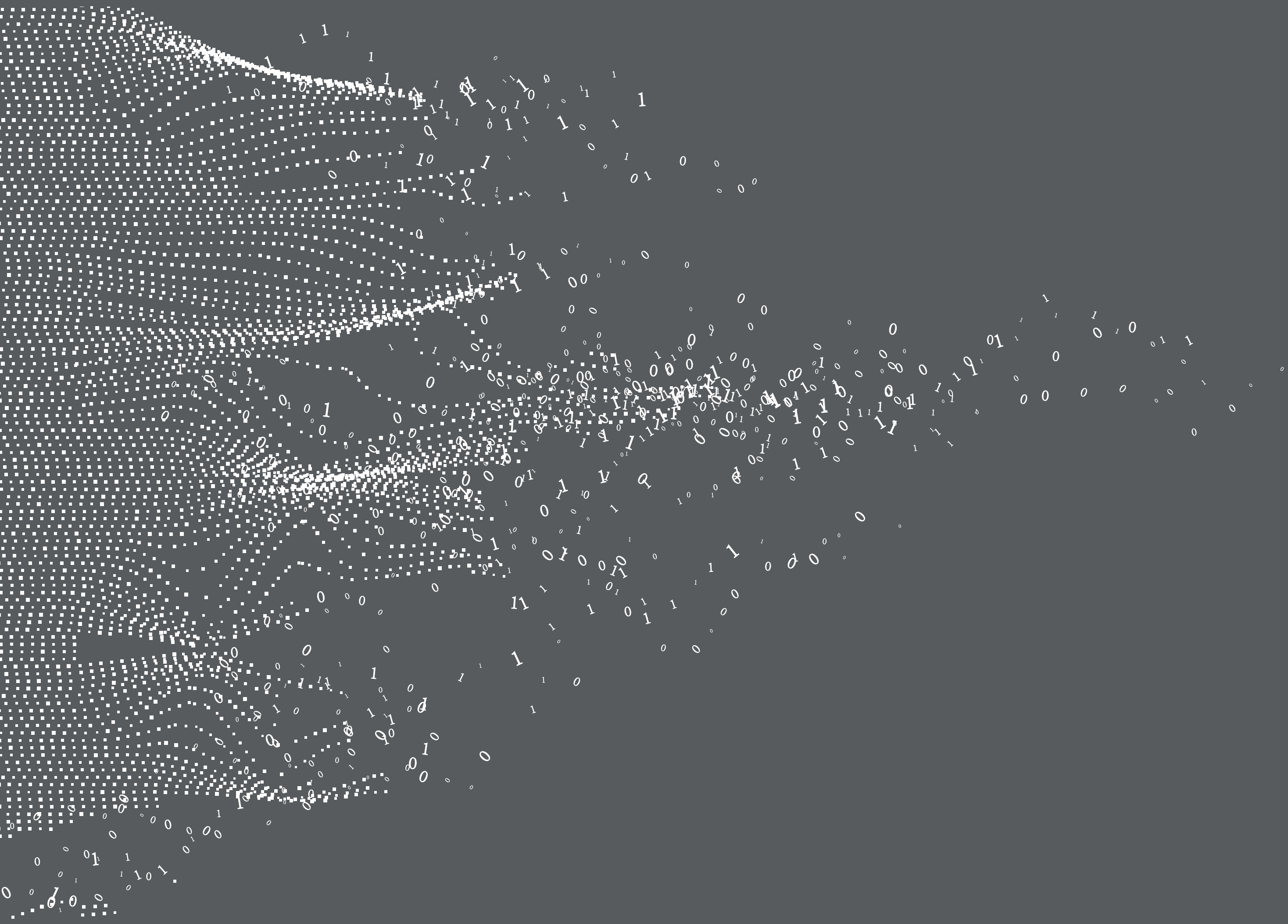
J.P.Morgan

A Merchant’s Guide to Preventing Card Testing Attacks



Safeguarding your business by combatting card testing attacks.

Card testing attacks are on the rise as fraudsters become more sophisticated in targeting e-commerce and m-commerce merchants. Now more than ever, merchants need to take proactive measures to protect their online business by adopting multi-layer security at checkout and enhanced fraud tools for detection and prevention. In doing so, they not only help combat card testing attacks, but also many other types of fraud gaining momentum in today’s environment.



What Is Card Testing?

Fraudsters attempting to verify illegitimately acquired credit card information.

Since fraudsters often identify valid cards prior to fraudulent activity, attacks can assume many forms with a few commonalities:

Acquire →

Obtaining full or partial card information from an illegitimate source such as:

- Data compromises and card data harvesting
- Stolen account information available via the dark web or brute force card data generation

Test →

Using stolen information (partial or full) at unsuspecting merchants to:

- Identify whether accounts are still active and not blocked by the issuer
- Try to derive missing card information based on the partial information stolen

Sell or Use →

Once card information is validated and active, fraudsters attempt to:

- Sell information on the dark web at a premium
- Initiate a maximum number of transactions (dollar amount) before the issuer closes the account

How does card testing work?

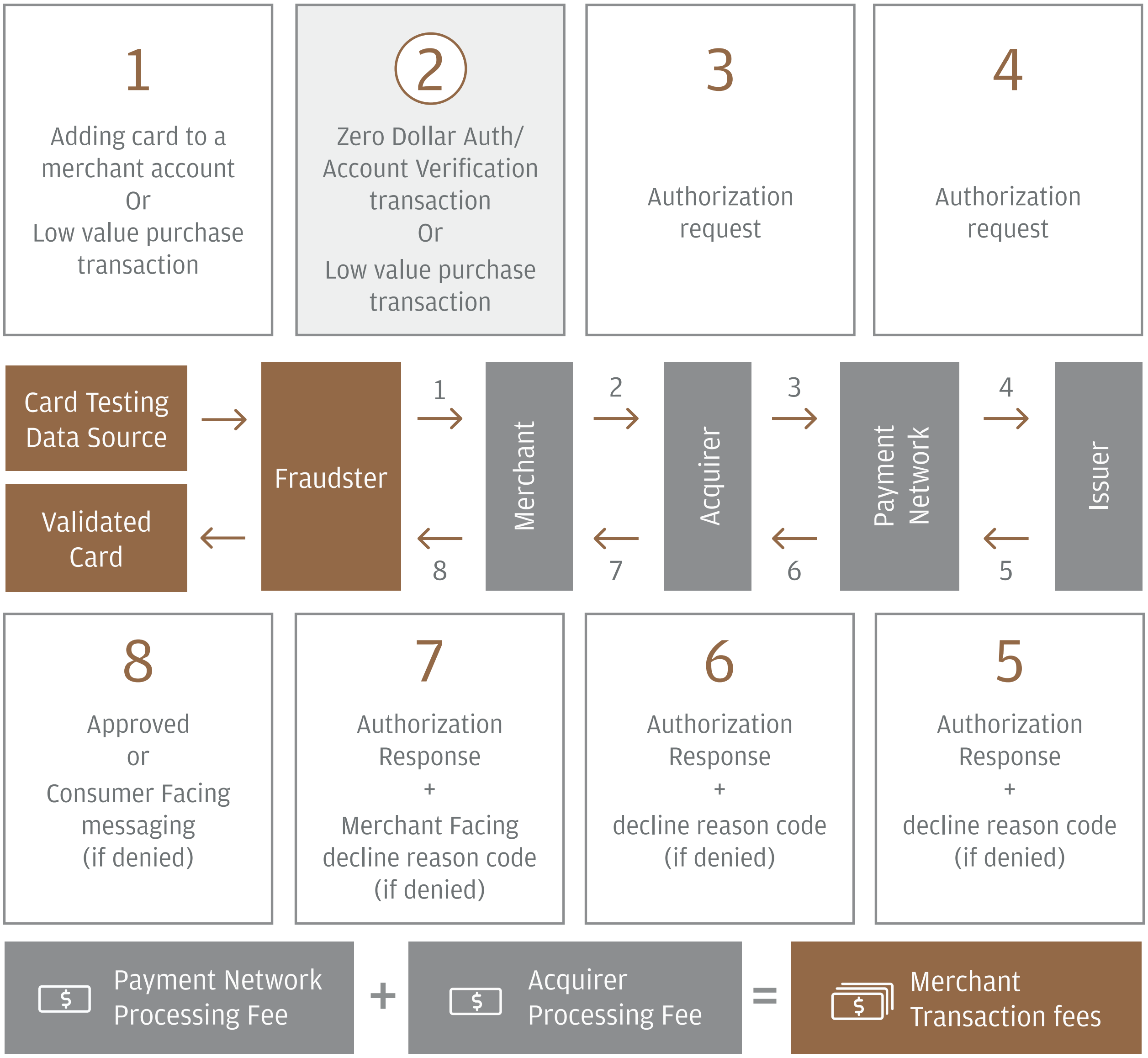
These attacks can be manual (low-risk, low-volume) or automated (easy, efficient and very attractive for fraudsters) depending on the level of sophistication. Automated attacks often pose a serious threat, causing significant damage to unsuspecting merchants.

The Transaction Flow of a Card Testing Attack

The goal of a card testing attack is to validate a card. To stop that, a merchant must prevent card testing before it reaches the acquirer (Step 2). If the merchant doesn't stop the attack, there could be financial consequences since merchant transaction fees would likely increase.

Based on the response, the fraudster may:

- Mark the card as valid
- Or adjust card info and resubmit again
- Or consider the card account invalid or
- Stop the attack if request is consistently denied without any info



1
Adding card to a merchant account
Or
Low value purchase transaction

2
Zero Dollar Auth/ Account Verification transaction
Or
Low value purchase transaction

3
Authorization request

4
Authorization request

Card Testing Data Source → Fraudster
Validated Card ← Fraudster

Fraudster → 1 → Merchant → 2 → Acquirer → 3 → Payment Network → 4 → Issuer

Issuer → 5 → Payment Network → 6 → Acquirer → 7 → Merchant → 8 → Fraudster

8
Approved
or
Consumer Facing messaging
(if denied)

7
Authorization Response
+
Merchant Facing decline reason code
(if denied)

6
Authorization Response
+
decline reason code
(if denied)

5
Authorization Response
+
decline reason code
(if denied)

Payment Network Processing Fee + Acquirer Processing Fee = Merchant Transaction fees

Who Is at Risk?

Web

E-commerce merchants that are not typically subject to high fraud due to the nature of their service or type of business, as they are often unequipped to defend against these types of attacks. Oftentimes, these merchants are not the actual target, but rather the mule or intermediate target being used in the process to obtain payment authorization and/or to determine if accounts are still active and valid

Mobile

Merchants using web, mobile web or mobile applications to operate their store fronts without the proper measures in place to detect and defend against card testing attacks

New to digital

Merchants new to the digital space and using the digital channel as a secondary store front

What merchants should know:

Card testing transactions are typically conducted with zero or small dollar values to avoid triggering fraud detection measures and raising suspicions.

When Do Attacks Occur?

Attacks are more frequent during peak seasons (i.e. holidays) for many reasons.

Fraudsters understand merchants lock down their environments during these times and deploying changes quickly is often not an option

High web traffic and transaction anomalies help hide attacks, slowing identification and discovery

Merchants might be hesitant to introduce or deploy untested/unproven changes in their shopping experience

Why Merchants Need to Pay Attention

Attacks that are not detected early and addressed promptly could have significant impacts on businesses, including:

- Increase in payment authorization fees
  - Acquirer/gateway transaction fees
  - Payment brand transaction processing fees
- Inability to support legitimate transactions
- Processing restrictions from payment networks
- Placement in high-risk programs, such as VDMP, VFMP and EFM
- Being treated as the potential source of fraud
- Payment authorization restrictions that could lead to potential false positives (good customers being declined)
- Being classified as high risk, which could trigger increased processing fees and merchant reserves
- High chargeback rates and fines

Keep in mind

Fraudsters try to avoid significant friction that could render attacks ineffective. Since they know merchants will eventually identify attacks and deploy temporary or long-term measures to protect their business, once met with resistance they will move on to easier targets.

How to Act

Merchants must have a comprehensive approach to defend against card testing. They can do so by using their own internal tools enhanced by external solutions, as necessary.

The solution is a multi-layer approach:

- Avoid becoming an easy target
- Merchants should introduce methods that exhaust fraudster's resources and cause increased expense to avoid practicing /testing on their business

Monitor all the merchant entry points through the cycle

- Purchase transactions
- Account creation
- Exception processing

Across all channels

- Web
- Mobile Web
- Mobile Apps

- Embed prevention measures and practices from the onset in the checkout experience and account creation flows, allowing the merchant to respond quickly
- Stop information leakage that can arm attackers with useful information to refine their attacks
- Plan to turn on additional measures to stop attacks and avoid impacting legitimate business

Keep in mind

Dispute details and the dispute response process is paramount to gaining insight into a business and fraud risks. If a merchant has a surge of disputes around small transactions, preventative measures should be put in place.

Monitor

Be on the lookout for:

- Higher volume of small transaction attempts
- Numerous purchases in a short duration
- High rate of authorization failures/declines
- Address Verification Service (AVS) alerts
- Card Verification Value (CVV) errors
- High volume of new merchant account creations
- Significant increase in the number of cards added to merchant accounts
- Consistent retries with different CVV2/CVC values
- New or constructed email addresses that seem suspicious
- Incorrect or repeated physical addresses
- Heavy volume from:
  - Specific IP addresses
  - Specific devices
  - Masked IP addresses using VPNs

Prevent →

Take steps to:

- Collect IP addresses and block attacking IP address ranges
- Require address verification service (AVS)
- Use velocity checks on easy to manipulate identity information (i.e. email and IP addresses)
- Use sophisticated device fingerprint technology
- Track bots and detect automated mouse clicks
- Throttle up transaction submission
- Protect the merchant environment and credentials

Respond →

Take cautionary steps to:

- Enable CAPTCHA, but use it with utmost caution
  - Intended to stop automated attacks by requiring a human to be a part of the flow.
  - Using a strong CAPTCHA can block automated attacks
  - Use with caution: CAPTCHA can create friction for legitimate users, as it degrades the user experience
- Enable user authentication, but balance it with the user experience
  - Intended to validate the consumers and help stop this type of attack from the onset
  - Provides merchant liability protection
  - Impacts on the user experience
- Blocking certain BINs may be useful in card enumeration attacks. But be careful, as you may be blocking good transactions

Review →

Continuously evaluate:

- Declined transactions
- Dispute data

Keep in mind

Do not rely on the chargeback process to identify card testing attacks. Long chargeback windows leave websites open to being hit multiple times before merchants are aware a problem exists. This can lead to numerous chargeback disputes and fees.

Discover How J.P. Morgan Safetech^{SM} Fraud and Card Testing Management Can Help

This enhanced solution enables a multi-layer defense that immediately recognizes signs of fraudulent activity and delivers accurate e-commerce fraud protection to help businesses improve bottom-line profitability.

- Checking signals that indicate automated attacks (i.e. customers with new email addresses and signs of bots)
- Protecting points in the customer journey with access to the payment system (i.e. web, app, phone, or other)
- Measuring velocities and linkage across multiple components of a purchase (i.e. device, IP, payment, address and phone)
- Identifying anomalies and inconsistencies in linked transactions
- Providing limited feedback to the card tester to make it harder for them to improve their techniques
- Recognizing automatically mass generated email addresses

How It Works

Safetech takes a multi-layered approach to prevent card testing attacks

1. Once an authorization attempt is made via website or mobile app, data is sent to Safetech for a risk inquiry prior to the issuing bank card authorization
   - Safetech's Identity Trust Global Network and adaptive Artificial Intelligence evaluates and generates a safety rating (i.e. Omniscore) and other key data points, allowing merchants to automatically assess trust level
2. If it is low, the authorization attempt is declined prior to being sent to the bank for authorization
3. If it is high, the authorization attempt is approved and sent to the issuing bank as an authorization request
4. Merchants can choose to auto-decision or decline low trust level authorizations, while enabling the merchant to avoid paying the authorization fees from the bank

Discover Safetech's Identity Trust Global Network

Empowering merchants with expansive cross-industry data curated from a diverse portfolio of digital e-commerce customers.

- Giving scores of fraud signals in real time
- Identifying suspicious authorization activity
- Detecting suspicious identities within your business

Learn more:

J.P. Morgan Payment Trends Report: Key Trends to Drive Your Payments Strategy

J.P.Morgan

This material was prepared exclusively for the benefit and internal use of the JPMorgan client to whom it is directly addressed (including such client's subsidiaries, the "Company") in order to assist the Company in evaluating a possible transaction(s) and does not carry any right of disclosure to any other party. In preparing this material, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was provided to us by or on behalf of the Company or which was otherwise reviewed by us. This material is for discussion purposes only and is incomplete without reference to the other briefings provided by JPMorgan. Neither this material nor any of its contents may be disclosed or used for any other purpose without the prior written consent of JPMorgan.

J.P. Morgan, JPMorgan, JPMorgan Chase and Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, "JPMC"). Products or services may be marketed and/or provided by commercial banks such as JPMorgan Chase Bank, N.A., securities or other non-banking affiliates or other JPMC entities and such affiliate or entity may or may not be the JPMC entity operating and regulated in your jurisdiction locally. JPMC contact persons may be employees or officers of any of the foregoing entities and the terms "J.P. Morgan", "JPMorgan", "JPMorgan Chase" and "Chase" if and as used herein include as applicable all such employees or officers and/or entities irrespective of marketing name(s) used. Nothing in this material is a solicitation by JPMC of any product or service which would be unlawful under applicable laws or regulations.

Investments or strategies discussed herein may not be suitable for all investors. Neither JPMorgan nor any of its directors, officers, employees or agents shall incur in any responsibility or liability whatsoever to the Company or any other party with respect to the contents of any matters referred herein, or discussed as a result of, this material. This material is not intended to provide, and should not be relied on for, accounting, legal or tax advice or investment recommendations. Please consult your own tax, legal, accounting or investment advisor concerning such matters.

Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMC and or its affiliates/subsidiaries. This material does not constitute a commitment by any JPMC entity to extend or arrange credit or to provide any other products or services and JPMorgan reserves the right to withdraw at any time. All services are subject to applicable laws, regulations, and applicable approvals and notifications. The Company should examine the specific restrictions and limitations under the laws of its own jurisdiction that may be applicable to the Company due to its nature or to the products and services referred herein. Notwithstanding anything to the contrary, the statements in this material are not intended to be legally binding. Any products, services, terms or other matters described herein (other than in respect of confidentiality) are subject to the terms of separate legally binding documentation and/or are subject to change without notice.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: https://www.jpmorgan.com/global/disclosures/interbank_offered_rates.

JPMorgan Chase Bank, N.A. Member FDIC.

JPMorgan Chase Bank, N.A., organized under the laws of U.S.A. with limited liability.