Citi Commercial Cards – Fraud Overview

2018 State of Texas Conference

Houston
October 2-3, 2018
University of Houston Hilton
4800 Calhoun Rd
Houston, TX 77004

Dallas
October 16-17, 2018
Doubletree by Hilton Hotel Dallas
Campbell Centre
8250 N. Central Expressway
Dallas, TX 75206

Austin
October 30-31, 2018
Commons Learning Center
J.J. Pickle Research Campus
10100 Burnet Road, Bldg. 137
Austin, TX 78758

Fraud

2018 - Strategic Initiatives & Observations

New Products

PEGA – Dispute Case Management Tool

Benefits

- Provide faster resolution to disputes raised
- Enhance future reporting capabilities
- Eliminate need for fraud affidavit

Timeline

- TS1 deployment scheduled for Oct 12th
- TS2 deployment scheduled for Jan '19

Enhanced Authentication

Lexis Nexis – One Time Passcode (OTP)

Benefits

- Enhanced client experience (high risk authentication)
- Reduced risk around Account Takeover scenarios – verifies cell # to c/h and ensures # hasn't been forwarded or ported

Timeline

- Full rollout in FEW by end of Sept '18
- Piloting in CS through Oct '18

Note: evaluating multiple vendors for various Biometric solutions as part of our long term strategy (utilization of voice, fingerprint and behavioral characteristics)

Recent Trends

Business E-mail Compromise (BEC) Attacks

- Discussed at Corp Conference
- Number of clients reporting attacks now up to 7
- Client communication drafted to raise awareness (scheduled to go out early Q4 '18)

Increase in misuse and abuse claims

To address clients should

- Review reports around spend occurring at legitimate MCC's, but outside of company policy
- Re-evaluate MCC Template and SPL
- Ensure proper approval process in place for expense reports and invoices

Fraud Lifecycle

Citi Fraud Management aims to mitigate all fraud types by leveraging clearly defined teams, working in tandem, in order to provide a holistic and safe solution for our customers

Fraud Analytics: Detection & Mitigation

1

Analytics

Analytics:

- Fraud analysis throughout the course of the day, evaluating unusual spend patterns and reviewing confirmed fraud cases
- Interact with Citi's partners and external working groups to identify compromised merchants

Strategy Development

Strategy Development:

- Rules created using a multitude of criteria:
  - High Risk Merchants
  - High Velocity Transactions
  - High Fraud Scores (provided by vendor and Associations)

Fraud Early Warning: Notification & Verification

2

Notification

Notification:

- C/H's are promptly notified via multiple channels (e-mail; SMS and Voice) when a fraud rule has been triggered

Transaction Verification

Transaction Verification:

- C/H can acknowledge charge is theirs – no further action required
- If Fraud charges are present will be provided with a toll-free number to call for further assistance

Security Operations: Recovery & Investigation

3

Recovery

Recovery:

- At point of notification c/h will be sent an affidavit that needs to be signed and returned to Citi for further processing – Note: credit will not be supplied until document has been returned
- Upon receipt of affidavit an investigator will be assigned to the case and all recovery efforts pursued

Citi's Fraud Strategy

What we are doing?
- Investing in industry leading models and tools to quickly detect data breach events

How it benefits you?
- Identify fraud sooner minimizing losses and cardholder impact

What are we doing?
- Chip and Pin cards
- 3D Secure
- Tokenization

How it benefits you?
- Blocks fraud at PoS
- Blocks online fraud
- Protects your data

What are we doing?
- Upgrading fraud models and rules engine

How it benefits you?
- Reduced cardholder declines at Point of Sale
- Improved false-positive and fraud detection rates

What are we doing?
- Investigate cases for potential misuse
- Maximize recoveries

How it benefits you?
- Identify employees using cards outside of policy
- Ensures that fraud charges are removed from your bill

What are we doing?
- Communicate timely and via multiple channels when fraud occurs (e-mail, voice and text)

How it benefits you?
- Reduced fraud declines and fraud claims
- Enhanced cardholder experience

Customer Contact Strategy

We have extended our communication channels to include voice, 2-way email, 2-way text and voice notifications, to help minimize cardholder impacts

Benefits to Clients

Security: Verify charges by replying to Citi's text message—free of charge

Timeliness: Receive immediate notification of suspect transactions for immediate action

Convenience: Confirm or refute suspicious activity immediately, even when traveling

Key Features

SMS and Voice

- **Two way text** and **voice message alerts** to potentially fraudulent activity on your account
- Two-way text allows cardholders to easily report fraud and approve transactions

E-mail Notice

- Our **one and two way e-mail notifications** are another way for you to stay in touch—whether you're at your desk, out of the office or traveling abroad

E-mail

- Sends e-mail to the cardholder
- Cardholder confirms or denies charge by calling Citi

SMS

- Citi sends Text Message (SMS) to the cardholder
- Cardholder confirms or denies charge thru SMS or by calling Citi

Voice

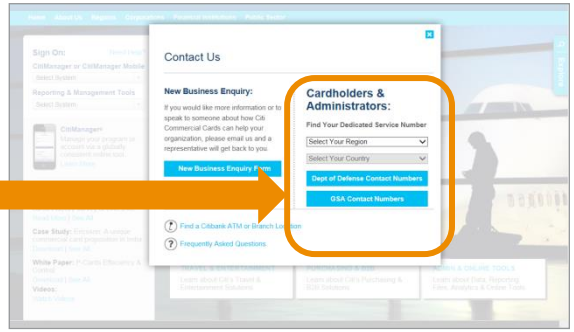
- Recorded system places call to the cardholder
- Cardholder confirms or denies charge during call with Citi

What to do if you Suspect Fraud

If you suspect any type of fraud, notify Citi immediately by calling the number on the back of your card

What Should I do if I Experience…. Fraud?

Call the general customer service number on the back of your card immediately. If you do not have your card, go to www.citicommercialcards.com, select the "Contact Us" button on the home screen, and enter your regional and country information for the appropriate Citi Representative contact number to call. Save the appropriate Citi number and information in your mobile phone contacts.



What Should I do if I Experience ….Phishing, Vishing or Smishing?

Report the suspected scam immediately to the following email addresses: spoof@citicorp.com. This ensures Citi is made aware of the potential scan and can conduct the necessary investigations. Within the US, also report the suspected scam to the US Federal Government at spam@uce.gov. If you have provided your account information or credit card number during one of these potential scams, please call a Citi Representative using the number on the back of your card or via the Citi website. The Citi Representative will close out your account immediately and have a new card issued to you.

What Information Should I Have Ready when Communicating with a Citi Representative and how can I be Sure that I am Speaking with Citi?

Citi will reach out to you via phone, text message and / or email, and a Fraud Early Warning block may be placed on your account. You will be asked to verify recent transactions (e.g. amounts and vendor names). **Citi will not ask you for any personal information during an outbound call.** If calling Citi back due to a message received (inbound call), we may ask you to verify your card number and / or additional details on your account (name, Employee ID, address, etc.). **Citi will NEVER ask you for your PIN.** If at any point during a Citi call you are not comfortable, the Citi Representative will understand and ask you to call the number on the back of your card or available via Citi's website.

Fraud Best Practices and Partnering with Citi

1. Ensure Citi **has current cardholder contact information** (cell, phone, and email)
2. Validate that your company's **email filters are configured to not block Citi Email**:
   - *Primary measure*: Clients should lower the spam score on mail from .citi.com, .citibank.com and .citigroup.com domains which pass DMARC. DMARC means the mail passes SPF, DKIM and has a matching visible sender and envelope sender
   - *Secondary measure*: You can whitelist the following IP Addresses with your email server 207.45.164.24, 207.45.164.79, 8.7.43.214, and 8.7.43.215
3. **Review accounts** tagged as fraud for employee misuse (liability waivers)
4. Place **temporary blocks** on accounts where c/h's are going to be on leave for an extended period of time.
5. **Cardholder education** - what to expect, review transactions, etc.
6. **Communicate** with Citi to ensure cards with fraud are shut down immediately
7. **Regularly look at your MCC's and credit limits**; Adjust velocity, credit and single purchase limits appropriately

Optimizing Your Program: Best Practices for Cardholders

Cardholders can use the below tips to help protect against fraud and avoid delinquencies, write-offs and late fees

1 Never Share your SafeWord™ Card or PIN

- Keep your card in a secure place, not out in the open
- Do not share your card with others. If you have a Chip and PIN card, never write or record your PIN anywhere
- When entering your PIN into a machine or ATM, use your free hand or body to shield the number from others' view

2 Practice Computer Best-practices

- Only install applications and software from well-known companies
- Use a pop-up blocker
- Log out and exit your browser or close the browser window
- Update browser and Java plug-in
- Password protect your computer and all accounts
- Do not leave passwords written or stored in an accessible place by others

3 Review Account Profile

- Confirm that your contact information (valid email address and mobile / cell phone number(s)) is up-to-date in the CitiManager account management tool, so that Citi can contact you quickly if needed
- Save the appropriate Citi number and information in your mobile phone contacts

4 Review Transactions

- Check your transactions online regularly and report unusual activity immediately

5 Shop Safely Online

- Only shop on secure sites that have a padlock symbol or have a web address that starts with "https"
- When using a Chip & PIN account, never provide your PIN details. The merchant does not need to know it
- Install anti-virus, anti-spyware and malware detection on your digital devices and keep them up-to-date

Note: Citi Commercial Cards will never share your information for marketing or commercial purposes

IRS Circular 230 Disclosure: Citigroup Inc. and its affiliates do not provide tax or legal advice. Any discussion of tax matters in these materials (i) is not intended or written to be used, and cannot be used or relied upon, by you for the purpose of avoiding any tax penalties and (ii) may have been written in connection with the "promotion or marketing" of any transaction contemplated hereby ("Transaction"). Accordingly, you should seek advice based on your particular circumstances from an independent tax advisor.

Any terms set forth herein are intended for discussion purposes only and are subject to the final terms as set forth in separate definitive written agreements. This presentation is not a commitment or firm offer and does not obligate us to enter into such a commitment, nor are we acting as a fiduciary to you. By accepting this presentation, subject to applicable law or regulation, you agree to keep confidential the information contained herein and the existence of and proposed terms for any Transaction.

We are required to obtain, verify and record certain information that identifies each entity that enters into a formal business relationship with us. We will ask for your complete name, street address, and taxpayer ID number. We may also request corporate formation documents, or other forms of identification, to verify information provided.