Protecting Your Commercial Card Program from Fraud - Webinar

August 13, 2020
Welcome

Fifth Third Bank

• Fifth Third Bancorp ("Fifth Third") is a diversified financial services company headquartered in Cincinnati, Ohio, in 1858.
• Fifth Third has $169B in assets. We are the 17th Largest Bank in the US.
• We operate 4 Main businesses: Commercial Banking, Branch Banking, Consumer Lending, Wealth & Asset Management.
• We operate 1,154 full-service banking centers.
• Third largest MasterCard issuer in the US.

Jon Hahner  Vice President, Senior Treasury Management Product Manager

• Over 9 years at Fifth Third Bank; 25+ years in payments industry leading strategic conversions/ implementations/ mergers/acquisitions, developing and supporting new product rollouts, and managing key client and vendor relationships.
• Commercial Card Product Manager; Prior role led the MB Financial merger card brand, network, and processor conversions for debit, consumer and commercial credit, and other card products.

Karen Cline  Vice President, Director, Fraud Product Risk Management

• Over 26 years at Fifth Third Bank within the payments realm focusing on Card Marketing, Product Management, Fraud and Operations
Agenda

• Background for Discussion
• Fraud Types, Sources, and Trends
• Structure of Fraud Management at Fifth Third
• Fraud Controls that Protect Your Portfolio
• Online Service Channels
• Future Enhancements
• Enhance Client Experience and Protect Your Card Program
• Questions/Answer
Background

- Card fraud losses worldwide were $27.85 billion in 2018, of which the United States accounted for $9.47 billion. While accounting for 21.54% of spend volume, US companies incurred 33.99% of the total worldwide fraud losses according to The Nilson Report. Fraud attempts will continue to grow and become more sophisticated as technologies advance.

- Payments Fraud impacts a great majority of organizations; Commercial card fraud is the third highest payment form impacted.

- In this session, you will learn of the various tools in place that help to identify and mitigate Commercial Card fraud losses along with discussions of upcoming technology changes and common sense steps that will improve the client experience and protect your card program.

Source: 2020 AFP Fraud and Control Report: Key Highlights
“Pressure from an economic crisis also affects employees and can make the company itself a [fraud] target.”

Bruce Dorris, President and CEO, Association of Certified Fraud Examiners (ACFE), March 31, 2020

“FBI reported increases in BEC fraud related to PPE and other supplies.”

FBI National Press Office, April 6, 2020

“Fast tracking new suppliers, focus on operational measures rather than compliance, and job cuts are providing fertile ground for fraudsters.”

Deloitte, April 10, 2020

“Fraud trends are rapidly emerging as bad actors look to turn a quick profit on the global pandemic.”

Forbes Magazine, April 10, 2020
Fraud Types/Sources/Current Trends

Types of Card Fraud
• Card Not Present (CNP) - Mail Order/Telephone Order, Online E-Commerce
• Counterfeit –Skimming (ex: Automated Fuel Dispenser)
• Stolen /Lost /Never Received
• Account Takeover – Phishing; Vishing; Business Email Compromise (BEC)

Sources of Payments Fraud- BEC, External, etc

Fraud Trends For Commercial Card Fraud
Q1 2020 Top 3 MCCs
  5542 - fuel dispenser automated
  7011 - lodging-hotels motels resorts-not classified
  5732 - electronic sales

Q2 2020 (based on what was reported within the same quarter)
  5732 - electronic sales
  5200 - home supply warehouse stores
  5542 - fuel dispenser automated

Source: 2020 AFP Payments Fraud and Control Report: Key Highlights
Managing Commercial Credit Card Fraud at Fifth Third

- Multiple teams work together to protect your credit card program from fraud
- Below are key functional topics in the fraud management process

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Analyze fraud trends and use industry leading tools to make enhancements to fraud rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevention Detection</td>
<td>Review current activity, monitor for suspicious activity, and communicate with cardholder</td>
</tr>
<tr>
<td>Recovery</td>
<td>Post-fraud event analysis including chargebacks, investigations, and SAR process</td>
</tr>
<tr>
<td>Intelligence</td>
<td>Industry networking to ensure best practices and partnership with law enforcement</td>
</tr>
</tbody>
</table>
Fraud Controls that Protect Your Card Portfolio

Card- Based Fraud Controls
• Chip Cards with Personal Identification Number (PIN)
• Card Activation
• Fleet card with Driver, Vehicle, or Generic ID input requirement
• Fifth Third ePay—single use virtual card numbers

Account - Based Controls
• Credit Limit
• Account Blocks/Statuses
• Merchant Category Code, Spend Limits, Cash Access Constraints
• Travel Notes

Process- Based Controls
• Authentication
• Fraud Detection/Suspicious Activity Calls
• Statement/ Transaction Review
Card Based Fraud Controls that Protect Your Portfolio (1 of 2)

• **Chip Cards with Personal Identification Number (PIN)**
  - Protects against skimming at POS devices
  - PIN requirement helps to validates the cardholder

• **Card Activation protects card while in transit to cardholder**

• **Fleet Cards setup with Driver#, Vehicle#, or Generic information in system**
  – When prompted at fuel pump, cardholder must enter the value that matches that information
  – Will see a wider requirement for PIN entry also as Fuel Pumps move to Chip readers

• **Fifth Third ePay– One Time Use virtual card numbers**
  - Ability to pay suppliers with a One Time Use card numbers with dollar, expiration, and merchant controls
  - ePay virtual card process is one of the most secure forms of payment
Value of Virtual Card (2 of 2)

Benefits of a Virtual Card

- Greatly reduces fraud risk
- Control over amounts and timing of payment
- Visibility into all card activity via online portals

Traditional P-Card

Virtual Card

Fifth Third Bank

A B2B solution from Mastercard
Account Based Fraud Controls

• Credit Limit on Account and Individual Cards
  – Ability to have various limits on individual cards
  – Mitigates risk of corporate level limit availability/exposure

• Account Blocks/Statuses
  – Ability for customers to suspend (turn off) cards if not required for use; ability to unsuspend at will
  – Used by a number of customers during COVID-19 period to turn off Travel Cards
  – TSYS (3rd Party Card Processor) ability to place certain Blocks real time based upon high risk transaction activity or confirmed activity
  – Customer confirmation interaction then typically required to remove Block

• Account Transaction Limits
  – Limit merchants at which card may be used by Merchant Category Code (MCC)
  – Ability to limit via amount or velocity (number of transactions) and limit cash advance access

• Travel Notes
  – Add specific notes regarding times/durations/locations of travel to assist when fraud agents review suspicious activity
Process-Based Fraud Controls

• Authentication/Verification

What is Authentication/Verification?
Process of confirming specific information for the Cardholder, the Card, and the Account to prove that caller is who they say they are and are authorized to discuss/change information on account.

When is it required?
- When calling to inquire on account/activity or respond to suspicious activity call or letter
- When calling to change/modify information if unable to do so via online channels

Why is it important?
- Allows authorized representatives to confirm identity in order to inquire on card, place blocks or remove blocks, or authorize other actions on the account
- Protects against fraudsters obtaining information or authorizing account changes
Process-Based Fraud Controls (2 of X)

• Detection/Suspicious Activity Calls
  
  – Fifth Third’s 3rd Party card processor, TSYS, utilizes industry leading fraud strategy and detection tools to combat monitor our programs and combat fraud.
  
  – TSYS executes outbound calls, to the phone numbers on the account, to reach cardholders/card program administrators to confirm whether a suspicious transaction is valid or fraudulent.
  
  - If contact not made at time of call, a message will be left to call TSYS at 855-634-1295.
  
  - The account may be Blocked until contact is made in order to protect the account.
  
  - If contact still not made, a letter may be sent, to the address on the account, requesting a call.

* This process is heavily dependent upon the quality of the Authentication/Verification information!
Process-Based Fraud Controls (3 of 3)

• Statement/Activity Review

– Fifth Third provides a monthly statements to Corporate and Individual Bill accounts

– Statements reflect the account balance, the payment amount information, and the detailed account activity

– Statements can be viewed via Fifth Third Direct (FTD) Commercial Card Management (CCM) portal or by cardholders in Cardholder Portal CHP

– If unauthorized or fraudulent transactions discovered, contact 800-375-1747

![Fifth Third Bank Statement Example]
Online Channels to Manage Your Card Program

Based on client need, four channels are used to support Commercial Card

Customer Needs

- Card administration
- Payments & expense management

Fifth Third Systems

- Commercial Card Management
- Card Holder Portal
- Card Payables
- Mastercard’s Smart Data g2

Commercial Card Tools

- Manage accounts
- Make Payments & manage suppliers
- Expense Management
- Transaction Reporting
- Alerts/Notifications
2- Way Fraud Alerts

- Real time fraud notifications to cardholder via SMS (text) and/or email
- Cardholder will receive text regarding suspicious transaction
- Cardholder will respond Yes/No or Valid/Fraud for further action
  - Yes/Valid allows spend to continue
  - No/Fraud blocks card and prevents further fraud
- Benefits:
  - Replaces the need to call into 1-800 number to confirm transactions
  - Mitigates interruption to additional spend; cardholder keeps using Commercial Card vs using personal card
  - Catches fraud quicker by blocking card in near real time.
- Target timeframe is Q1, 2021
- Phone Number Campaign target for Q4, 2020
Commercial Card- Future Enhancements

One Time Password (OTP)

- Ability to send an OTP to a verified phone number via SMS text or via a phone call
- Premise is to verify the identity of the caller requesting the information or requiring the action
- Use cases and implementation approach being developed
- OTP is dependent upon the 2 Way Fraud Alerts Phone number gathering Campaign
- Target timeframe for implementation is Q1-Q2, 2021
Enhance Client Experience and Protect Your Program

- **Access to the Online Systems to Manage your Program’s Accounts via Fifth Third Direct**
  - Commercial Card Management (CCM)
  - Cardholder Portal (CHP)

- **Ensure Authentication/Verification information is Present and Accurate on Accounts**
  - Verification challenges are probably our #1 Issue
  - Process driven by information on system, but must be known by Cardholder/Program Admin
  - Information consists of a 3 factor combination for Verification process – Card, Cardholder, and Account
  - Two pieces of information are the most prevalent reasons for not passing Verification
  - Have Phone numbers that are useful to be able to actually reach an individual
    - Especially relevant in this COVID environment
    - Ex. Main office or hardline numbers without routing/receptionist

- **Suspend cards that are not in Use**
  - Protects against unauthorized charges, accidental use, or credit master type attacks
  - A number of organizations have done this during COVID and low T&E travel time
Enhance Client Experience and Protect Your Program (2 of 2)

- Utilize MCC controls, amount and velocity controls, and credit limits
- Place Travel Notes on Account as additional information for fraud review
- Establish Alerts in Fifth Third Direct Ex. Notice of accounts blocked for suspicious activity, reported lost stolen, etc
- Review statements/transaction activity and notify Fifth Third if dispute
- Sign up for Fifth Third ePay to pay suppliers with one time use virtual cards vs traditional P-card
- Reinforce your internal training, card policies and procedures, and audit and program reporting
- Support our upcoming Phone Number gathering campaign to enhance the Verification experience
Questions?

Thank you.

Contact Info:

Email: jon.hahner@53.com