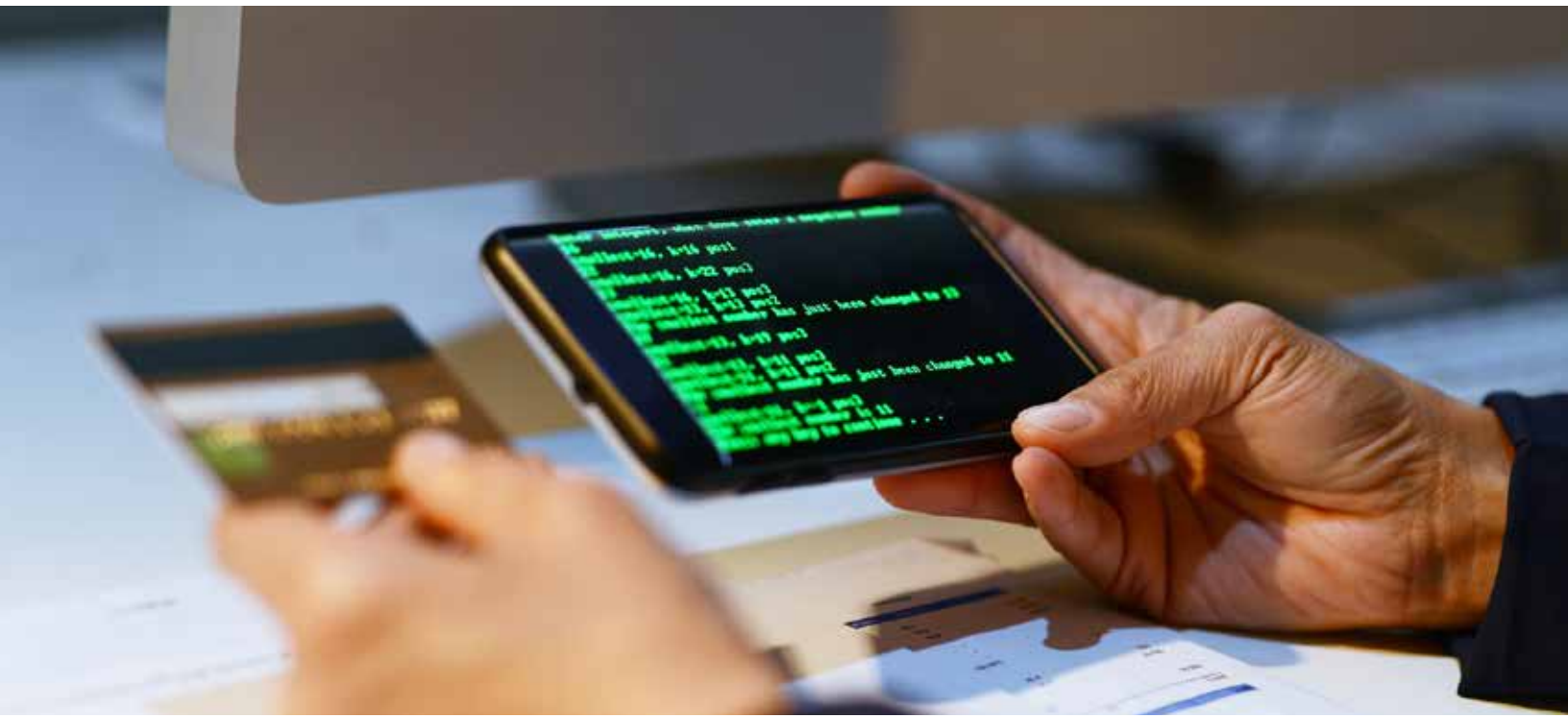
COMDATA®
CORPORATE PAYMENTS

Reduce Fraud with Comdata Commercial Cards

WHITE PAPER: REDUCE FRAUD WITH COMDATA COMMERCIAL CARDS

In the age of technology, payments-related data breaches can happen to even the most secure financial institutions. They can happen internally or externally, and in various formats. According to Investopedia, fraud is, "...an intentionally deceptive action designed to provide the perpetrator with an unlawful gain, or to deny a right to a victim." The extracted data is commonly used to commit card fraud.

As Experian puts it, "Credit card fraud is when someone uses your credit card or credit account to make a purchase you didn't authorize." The most common type of fraud is external fraud, which involves lost, stolen, or counterfeit card or account information used to make purchases in person or online, per the Mercator Advisory Group. External fraud originates from third parties, such as merchants and contractors that can range from a lone perpetrator to experienced crime rings. Though external fraud is most common, internal fraud generates the most revenue losses. US Legal defines internal fraud as fraud that is committed by an individual against an organization. "In this type of fraud, a perpetrator of fraud engages in activities that are designed to defraud, misappropriate property, or circumvent the regulations, laws, or policies of a company." (US Legal) It is, "...one of the widest reaching fraud typologies, spanning many departments, roles, processes, and systems." (SAS)

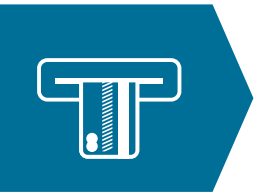


Types of Data Breaches

External fraud on payment cards commonly occurs through data breaches. Data breaches usually involve more than one way of attack, but all breaches have one or two things in common: gaining personal/identity information and/or financial data. There are four main types of data breaches:

System/Network Attacks

Network system attacks, including Point of Sale (POS) attacks, succeed as data breaches when a security weakness allows harmful software to enter. Attacks can be active (hacker actively seeking information by introducing foreign data or programming) or passive (hacker monitoring and/or collecting information on the network activity). "If a card account has potentially been compromised through a data breach, the issuer might proactively close it and reissue a card, or, if no fraudulent attempts have occurred, simply monitor it." (Mercator)



Card Skimming

Remember in Terminator II: Judgement Day where a young John Conner and his friend use a hand-held device to get money out of an ATM? That, my friends, is card skimming. And there's more than one way to do it! These devices can be installed over a card reader, paired with a camera to capture a cardholder's personal identification number (PIN).

Phishing

Have you ever received a strange phone call or email from a company asking for personal information? They want to know about a username or password, answers to common security questions, social security numbers, account numbers, or card credentials. This is phishing, the act of tricking people into revealing sensitive information. Scammers may use emails, calls, websites, and now even texts (SMSishing) to get people to share valuable information. They use logos of established and familiar companies or pretend to be a family member. Their main goal is to steal money or identities.

Types of Data Breaches (cont.)

Business Email Compromise (BEC)

BEC fraud typically occurs at companies that work with foreign businesses or suppliers that regularly send payments through wire transfers. BEC involves social engineering, identity theft, email spoofing, and even the use of malware. According to the FBI, "...scammers target employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners." The money, though, ends up in accounts controlled by scammers.

Additional Types of Data Breaches

ATM Fraud

Commercial cards generally do not allow access to cash because the employer loses control of spending when the employee uses cash, but there are a few helpful applications for cash access such as expense reimbursement or cash advances. Comdata offers a Cash Wallet feature for customers to accommodate these exceptions. When using your card at an ATM make sure your PIN is safe from view and never share your PIN with anyone. Ensure a skimmer has not been installed by nudging the card slot and verifying that the keypad has not been compromised. If you find that an ATM has been compromised, notify the ATM's bank immediately and do not use it to withdraw any funds or check the balance of your account.

Fuel Fraud

Fuel fraud from card skimming is on the rise because automated fuel dispensing point of sale devices represent the largest holdover of merchants moving from magnetic stripe to chip card support and fraud always follows the weakest technology. Such exposure should decrease when a liability shift takes effect in October 2020, and merchants who remain without chip support after the liability shift will experience increased chargeback loses.

In addition to external fuel fraud, drivers may misuse company funds for their own personal gains. To mitigate misuse of funds, lower spending limits, require strict prompts, review invoices frequently, segregate duties with appropriate checks and balances, and recommend cardholders to always swipe their cards instead of manually entering information when making a purchase. Also, lock cards down to specific MCCs (merchant category codes) so they cannot be used for non-business related purchases.

WHITE PAPER: REDUCE FRAUD WITH COMDATA COMMERCIAL CARDS

Commercial Cards

VS

Consumer Cards

There are two types of credit cards used by companies: Consumer (personal) and Commercial. Commercial cards are typically referred to as business or corporate cards depending on the market segment to which they apply. For example, small businesses may refer to commercial cards as business cards while larger corporations may refer to them as corporate cards.

Commercial cards have more control over spending, greater flexibility, more customizability, and are centrally managed. Most importantly, commercial cards offer direct data feeds. Direct data feeds integrate card use with fleet or expense management systems, such as Comdata's Expense Track which allows customers to generate, submit, and approve expense reports.

At Comdata, we offer commercial cards backed by Mastercard for all your purchasing needs. One important difference to note between Mastercard consumer and commercial cards is their Zero Liability Protection. While Mastercard does not hold consumer cardholders accountable for unauthorized transactions, the Zero Liability Protection does not apply to commercial cardholders with the expectation that they are able to hedge potential loses through participation in interchange revenue (i.e., rebate).

Interchange is meant to include reimbursement to issuers for risk costs, which is why companies share the loss on fraud transactions since they receive rebates from the interchange that we receive on your transactions. Comdata pays for the transaction program and processing costs (authorization, clearing/settlement, etc.). In addition, you, the commercial card customer, are responsible for unauthorized charges with a few limited exceptions.

Who is the Victim of Fraud?

Typically, fraud is perceived as affecting only cardholders. However, in the commercial card industry, the cardholder, or employee, has little to no personal data exposed. Instead, your company and the card issuer are affected by fraud in the commercial card industry. Your company is liable as they are responsible for unauthorized charges. The card issuer risks reputational damage, and the credit limits and exposure of corporations far exceeds that of a consumer cardholder.

How Comdata Can Help You

At Comdata, we provide many options for protecting you and your cardholders from fraud, whether it be internal at your company or external through data breaches. Take advantage of these features to ensure your commercial card program is safe and successful.

Increased Controls

Enhanced Visibility

Security of the Mastercard Network

Fraud Prevention Best Practices

Protecting your business's cardholders from fraud and identity theft is top priority at Comdata. "...one of the largest contributors to internal card fraud and policy violations is poor oversight," says the Mercator Advisory Group, which is why Comdata takes the necessary precautions toward fraud prevention. See below for information on Comdata's fraud prevention tools.

IBM Safer Payments

Safer Payments is Comdata's fraud detection system that uses artificial intelligence and rules based technology to identify suspicious patterns in transaction activity. Safer Payments monitors all authorization requests from all transactions in real-time. Safer Payments declines transactions if they fall into predetermined fraud patterns understood by the system, and can approve transactions that may be suspicious for follow-up with the company administrator or cardholder. Safer Payments comes at no cost or additional sign up.

Alerts and Notifications

By signing up for Comdata Mastercard commercial cards, you have immediate access to Alerts and Notifications (A&N), one of Comdata's most popular fraud prevention tools. A&N is available in the US and Canada. Note that A&N applies to only driver/employee cards, not vehicle cards at this time.

With A&N, your cardholders can continue using their cards even after fraud is detected. Any time Comdata's fraud detection system identifies a suspicious transaction, your cardholder receives a text alert asking them to validate the transaction. Then, your cardholder can reply to the message confirming whether or not the transaction was fraudulent. If the cardholder confirms fraud, the card will go into a locked-down state and each additional transaction will be declined. However, the cardholder will receive a text message with each declined transaction allowing them to override the decline. If they override, they can swipe/dip their card again and continue the transaction as normal, as long as the transaction is for the same amount and from the same merchant. If the cardholder receives a declined transaction they don't recognize, there's no need to respond as the transaction was not authorized.

As an optional benefit to A&N, you can also elect for your cardholders to receive text notifications if a card is declined for non-fraudulent activity, such as a transaction that exceeds daily limits or a cardholder attempting to use their card at an unauthorized merchant. Based on the reason, you or the cardholder can take corrective action so the transaction can process. The text notification reduces company overhead in cardholder inquiries to your program administrator.

Fraud Prevention Best Practices (cont.)

Expense Track

Expense Track is Comdata's expense management system that allows you to generate, submit, and approve expense reports. With Expense Track, each time one of your cardholders swipes/dips their card, their transaction details are fed into the system and populated on an expense report. You can then go in and review the transaction before approving it for reconciliation. If a transaction seems suspicious, you can decline it within the approval process and research it further to determine if it was fraudulent or legitimate. Note that this does not decline authorization of the transaction, but rather declines it for expense approval. Your company policy may require the cardholder to reimburse the company for fraudulent expenses. The convenience and ease of processing expense reports adds immediate recognition of unauthorized activity.

Authorization Controls

As a card program administrator, you can set controls around the usage of cards, such as daily spend limits, daily transaction limits, and purchasing limits. You can even lock cards down to specific MCCs (merchant category codes) so that cardholders don't misuse funds. For more information about authorization controls, contact your Comdata Account Manager.

EMV (Europay, Mastercard, Visa) Chip Cards

EMV chip cards have led the way to fraud prevention at point-of-sale (POS) devices. Traditional credit cards use a magnetic stripe on the back of the card which stores all pertinent data to the cardholder. Information on the magnetic stripe is static which means it will never change. Fraudsters skim this static data to create counterfeit cards.

With EMV chip cards, the cardholder's data is still stored in the magnetic stripe, but also on the chip which generates a unique code each time a transaction occurs. The code restricts fraudsters from performing fraudulent transactions with the cardholder's data when the chip card is dipped or inserted at the POS device.

Fraud Prevention Best Practices (cont.)

iConnectData (ICD)

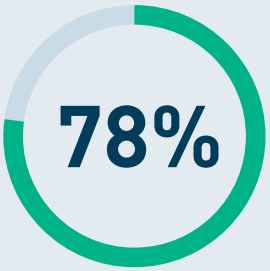
ICD is Comdata's account management portal where you may spend most of your time managing your commercial card program. ICD provides a secure login that requires you to select a username, password, image, and image caption. ICD will display your chosen image and caption each time you log in. If not, contact a Comdata representative immediately as this may be a fraudulent website.

For extra security, Comdata has teamed with IBM to offer Trusteer Rapport, an online IBM fraud protection software available to you free of charge. Trusteer Rapport operates with any other anti-virus software installed on your computer and helps prevent financial malware and fraudulent websites from stealing your online IDs. Trusteer Rapport provides warnings if you accidently visit a fake website and malware is downloaded. For more information on adopting Trusteer Rapport for your company, contact your Comdata representative.

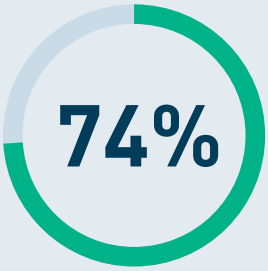
Virtual Payments

According to the 2018 AFP (Association of Financial Professionals) Payments Fraud and Control survey, 74% of organizations experienced fraud via checks in 2017. Fraud was committed on not only paper checks, but also electronic checks via BEC. The survey also states the majority of fraud payments organizations experience centers around checks and the majority of check payments are issued electronically.

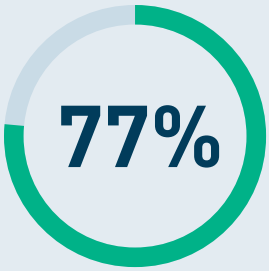
With Comdata, you have access to an electronic payment solution in the form of single-use virtual cards. Virtual cards are 16-digit Mastercard numbers that can be transferred electronically to a payee over the secure Comdata network. Single-use virtual cards have proven to be more secure than traditional forms of payment, such as checks and even plastic cards.



of companies reported fraud last year



of companies reported their check payments were exposed to fraud



of companies experienced fraud via Business Email Compromise (BEC)

**source: AFP*

Additional Fraud Prevention Best Practices

The following are additional best practices for preventing fraud:

- Use ICD to view your transactions and maintain your cards.
- Comdata will never call and ask for your ICD login information or your code word (security code or passcode).
- Do not give anyone personal/business information.
- Use a strong code word and password and do not give them to anyone
- Update your code word as employees change.
- Ensure your list of employees with account access is current and accurate.
- Review user profiles and limits.
- Do not use shared logins; every user must have their own login.
- Block a card when you discover it will no longer be used (employee leaves company, is lost or stolen, unit is no longer in service, etc.).
- Set appropriate daily/weekly limits that meet the spending needs of your cardholders.
- Establish security for card administrators and keep it up to date as roles change or people leave the company.
- Secure your cards and only assign them to employees as needed.
- Set reasonable product limits.

What to do When Fraud is Suspected

If cardholders suspect fraud, they should report it to you immediately. Then, you must contact Comdata to let us know their card has been compromised. Once a card is reported as lost/stolen, your company is no longer responsible for fraud committed on the card. You should also file a dispute report when fraudulent charges have been made due to a compromised card via the ICD Online Dispute Form. Refer to the ICD Resource Center for more information about the dispute form.

As a Comdata commercial card user, you also have access to the MasterCoverage Liability Protection program which is designed to protect against internal cardholder misuse. With MasterCoverage, your cards are insured if internal employees misuse them for personal gain. See the MasterCoverage brochure on the ICD Resource Center for more information.

How Cardholders and Companies Can Work Together

As program administrator, there are many methods you can take to ensure cardholders are aware of fraud prevention, such as:

- Educate your cardholders on the role they play in A&N.
- Ensure travel policies are current and distributed annually.
- Require cardholders to acknowledge travel policies by requiring them to read and confirm their acknowledgement.
- Ensure cardholders are trained on how and where to whom to report suspicious or fraudulent activity or lost/stolen cards.

You should also review and analyze transactions and user activity on Expense Track and ICD, such as declined transactions, new accounts, closed accounts, invoice review, etc.

Conclusion

Although card fraud can occur, you have access to a number of fraud prevention products and tools as a Comdata customer. Using Comdata's fraud prevention suite of products mitigates risk of fraud for your cardholders, reduces financial loss due to fraud, and allows cardholders to travel safely knowing their expenses are secure. If you are not using one of the fraud prevention products mentioned here, contact your Comdata account manager today to get started.

Frequently Asked Questions by Comdata Customers

1. Will any of Comdata's fraud prevention tools incur a fee?

No, all of our fraud prevention tools are provided free of charge! However, note that standard rates apply to text messages received in the A&N program.

2. What should I do if I see a posted transaction that is not mine?

Review your Real Time Transaction History through iConnectData (ICD) or Expense Track. Once you have verified the transaction is not yours, block the card immediately. When possible, reissue the card through ICD. For help, immediately contact your Comdata account representative.

3. What is a Force Posted transaction and can it be charged back?

A Force Posted transaction settles without the merchant obtaining an authorization from the issuer. Anything that is force posted can be charged back subject to rules in place by Mastercard. Note that fewer than .001% of transactions are force posted.

4. Are there chargeback rights if a transaction, or the amount, is not valid?

Yes, however, the issuer does not know what has happened between the cardholder and the merchant from the time of authorization to the time of settlement. Mastercard says, "The issuer must try to honor the transaction before exercising the chargeback." Therefore, it is important that you notify us about any transaction disputes within 60 days of the suspicious charge.

5. Once I confirm that a transaction is fraudulent, is the new card automatically reordered?

No, Comdata is responsible for ensuring the card is blocked when fraud is confirmed, but not responsible for card replacement. You will need to order a new card or contact your company Administrator/Manager to have one ordered for you. The company Administrator/Manager makes the decision whether or not to reorder the card for the cardholder.

6. When I dispute a transaction, how long does it take to receive the corresponding credit?

No more than 30 days. Note that this credit is provisional pending the resolution of the dispute through Mastercard. If the dispute is unsuccessful, the credit will be removed.

7. Can I see the status of my dispute in iConnectData (ICD)?

We can provide you access to the Mastercard Dispute Report, which is available in ICD reportQ. This report allows you to download disputes and view their statuses.

8. Do I have any recourse if any of my employees commit fraud with their corporate card?

Yes, Mastercard offers the MasterCoverage Liability Protection program. With MasterCoverage, approved claims reimburse you for any funds lost due to internal employee misuse. Contact your Comdata commercial card representative for more information.

WHITE PAPER: REDUCE FRAUD WITH COMDATA COMMERCIAL CARDS

About Comdata

For nearly 50 years, Comdata has been a leading provider of innovative B2B payment and operating technology. By combining our unique capabilities in technology development, credit card issuing, transaction processing and network ownership, we help our clients build electronic payment programs that positively impact their bottom line and operate their businesses more efficiently. We continuously evolve our products by focusing on our customer's needs to provide security, accessibility, and profitability.

As a division of FLEETCOR Technologies, Comdata is part of one of the largest payment companies in the world and is the second largest commercial issuer of Mastercard in North America. Our employees partner with companies in 53 countries to manage more than 1.9 billion in fleet, corporate purchasing, payroll and healthcare transactions annually.

CORPORATE PAYMENTS

www.comdata.com
1.800.COMDATA
payments@comdata.com

References

"Business E-Mail Compromise." FBI, FBI, 27 Feb. 2017, www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise.

Chen, James. "Fraud." Investopedia, Investopedia, 13 Dec. 2018, www.investopedia.com/terms/f/fraud.asp.

Hall A, Richard. Fighting Commercial Card Fraud and Bringing the Information Gap. Fighting Commercial Card Fraud and Bringing the Information Gap, Mercator Advisory Group, 2015.

Lupovici, Jessica; St Jean, Bob. 2018 AFP Payments Fraud and Control Survey. 2018 AFP Payments Fraud and Control Survey, J.P. Morgan, 2018.

SAS (Statistical Analysis System). "Internal Fraud - The Threat from Within." Internal Fraud White Paper PDF, 11 Aug. 2014, www.sas.com/content/dam/SAS/da_dk/doc/whitepaper1/Internal%20Fraud%20Whitepaper_SAS%20Institute.pdf

US Legal, Inc. "Internal Fraud Law and Legal Definition." Fraud Law and Legal Definition | USLegal, Inc., definitions.uslegal.com/i/internal-fraud/.