BBVA Compass
Creating Opportunities

Preventing Payments Fraud

Helpful Hints

Table of Content

This document is provided for informational purposes only. Nothing in this document shall be considered, or relied upon, as legal, regulatory or operational advice. All references to external documents or websites do not constitute an endorsement or an approval by BBVA Compass of any of the products, services or opinions of the corporation or organization or individual. You should consult your own legal counsel for further clarification.

BBVA Compass is a trade name of Compass Bank, a member of the BBVA Group. Compass Bank, Member FDIC.

Introduction

#1 Mistake People Make When They Are Victims of Payment Fraud

People are sometimes embarrassed when payments fraud occurs, and they don't want anyone to know they were vulnerable. But **initiating fraud investigations without notifying your bank(s) is a big mistake** as you may unknowingly compromise your bank's ability to recover funds on your behalf.

6 Tips to Strengthen Passwords

92% ***of online users use the same password across multiple accounts***

which puts all of your data at risk. Here are 6 tips to make sure your passwords are as strong as possible.

Make passwords as long as possible

A 16-character password would take 22 billion years to crack, 3-character passwords take 1 second to crack.

Change your passwords regularly

The more sensitive the information, the more often you should change your password.

Include numbers, symbols and letters

Randomly mix up symbols and numbers with letters. Substitute zero for the letter O.

Avoid using obvious personal information

Select security questions and answers that would not be discoverable by browsing social media accounts.

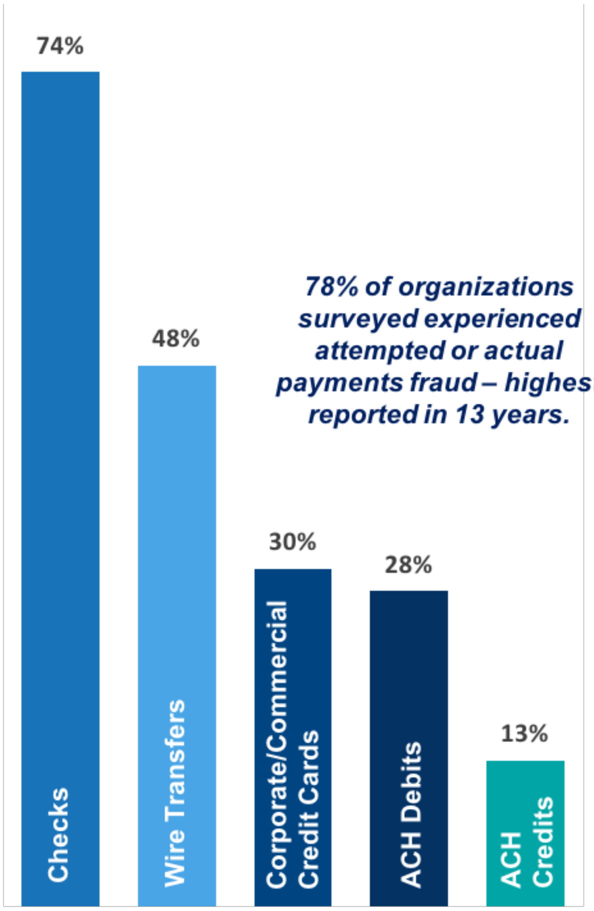
Do not reuse passwords

Use unique passwords for everything to minimize exposure in the event your account is compromised.

Start using a password manager

These are services that auto generate and store strong passwords for you in an encrypted, centralized location that you access with a master password.

It is **critical to contact banks on all suspicious activity immediately**, so that the banks can take actions to contain the incident.



78% of organizations surveyed experienced attempted or actual payments fraud – highest reported in 13 years.

Source: 2018 Association for Financial Professionals (AFP) Payments Fraud & Control Survey

Best Practices for Individuals

10 Ways to Secure Your Mobile Phone

We often use our phones for two-factor identification and password resets, but hackers can take control of your phone number and transfer it to a new phone that they control so that your secure verification codes go to them. Here are some steps that will make you a harder target.

- ***Change factory passwords on your phone*** and do not use 0000, 1234 or your birthday. Avoid settings for auto-login or saving passwords.
- ***Install app and system updates as soon as they are available*** because these updates may be fixing a bug or security issue.
- ***Only download apps from the App Store, Google Play, or other official sources***, as they constantly screen and remove suspicious apps.
- ***Do not access sensitive information (such as bank accounts) while using unsecure public Wi-Fi.***
- ***Set your phone's lock screen feature to engage quickly when the phone is not in use.***
- ***Set your phone to auto-erase if too many incorrect logins are attempted*** (and make sure to back up your phone regularly).
- ***Turn off your phone's Bluetooth feature when not in use.***
- ***Enable the "Find my phone" feature*** so that you can quickly locate it if it is lost or stolen.
- ***Turn off your devices when not in use*** (do not just hibernate them), especially when travelling.
- ***Install privacy screens for your devices.*** These are tinted screens that prevent bystanders from seeing what's on your screen.

3 Online Habits to Consider

Prudence when using the internet pays off in the long run.

- ***Never submit financial information through a website that does not have multi-factor authentication (MFA).*** MFA is an effective deterrent to external fraud because it is unlikely that a perpetrator will have all the factors needed to commit fraud:
  - Something the user knows (e.g., password, PIN);
  - Something the user has (e.g., ATM card, smart card); and
  - Something the user is (e.g., biometric characteristic, such as a fingerprint).
- ***Avoid using automatic login features that save username and password for online banking.*** This information is stored in "cookies" during internet sessions and could be retrieved if a computer is compromised.
- ***Log out.*** Be sure to log out before you end the session. Logging out will invalidate session cookies so that no information remains available to the next user or hacker.

10 Worst Places to Use Public Wi-Fi

Connecting to an unsecured, free, public Wi-Fi hotspot exposes you to countless security threats because **public networks are extremely vulnerable to hacks.** Using tools such as Wireshark, hackers can intercept email, listen to VOIP conversations, read IM's and otherwise enjoy your traffic, including stealing cookies to authenticate themselves as you use websites. ***It is substantially safer to use the hotspot on your mobile phone than to risk using public Wi-Fi.*** If you must use a public Wi-Fi hotspot, try to avoid these places:

- Airports
- Hotels
- Public Parks
- Restaurants and Fast Food Places
- Coffee Shops
- Stores
- Public Library
- Hospitals
- Municipalities / Cities Hotspots
- Trains/Buses

Protecting your Company

6 Types of Positive Pay Services

90% of organizations surveyed by AFP's 2018 Payment Fraud and Control Survey reported that they use Positive Pay to guard against payments fraud.

ACH Positive Pay

Matches incoming ACH debits and/or credits against established business rules to determine which trading partners are allowed to debit your account(s) with some banks offering the ability to build business rules from incoming transactions. Discrepancies are reported to you for a pay or return decision.

Check Positive Pay

Compares the check number and dollar amount of the check presented for payment to the information in your check issue file. Discrepancies are reported to you for a pay or return decision.

Deposit Positive Pay

Used for Deposit-only accounts, you can receive notification every time a check is presented for payment on the account(s) and ask you for a pay or return decision. This is popular for customers with multiple locations or departments depositing into a single account which is widely known and very vulnerable to check fraud.

Payee Positive Pay

Looks at the payee name in addition to the check number and dollar amount when comparing the check presented for payment to the information in your check issue file. Discrepancies are reported to you for a pay or return decision.

Reverse Positive Pay

Transfers the burden of comparing checks presented for payment against the check written to the company who must then notify the bank of any discrepancies.

Teller Positive Pay

Extends Check (and sometimes Payee) Positive Pay protection to the branches to review checks presented by payees for encashment or deposit against your issue file. For many banks, this service is included with Check and/or Payee Positive Pay at no additional cost.

5 Ways to Decrease Card Fraud

- ***Define card spending limits by employee*** **or by employee level** to correspond with their responsibilities.
- **Conduct a monthly management review of compliance with card usage policies and procedures.** A permanent oversight function is a strong deterrent to internal fraud.
- ***Consider separation of duties for submission of new card requests and the receipt of the physical card*** to prevent unauthorized account setup. Consider doing this for payments to the card issuer to ensure legitimate payments.
- ***Deploy EMV (chip-enabled) terminals for card payments at customer facing locations.*** The Nilson Report determined in October 2017 that losses decreased by 60% compared to 2014 at merchants who used chip-enabled terminals. Criminals have yet to successfully create counterfeit cards with EMV chips.
- ***Check security settings to ensure address verification (AVS) is turned on.*** (If you have an online store) Companies are often elated to have their decline rate on credit cards at zero, but this is not normal. If your dispute rate is high (average dispute rate is under 1%) but you have a zero-decline rate, this usually means that fraudsters have discovered a loophole in your settings and are exploiting it.

3 Practices to Protect Against ACH Fraud

Fraudulent debits against business accounts is the second (first is consumer accounts) most frequent attack for ACH payment fraud, according to the Federal Reserve Bank of Minneapolis. To limit the occurrence of ACH fraud, companies are implementing measures such as these:

- **Reconcile accounts daily so that unauthorized ACH debits are identified and returned timely** 69% of AFP 2018 survey recipients implemented this practice. NACHA rules require that unauthorized or improper corporate debits be returned no later than the opening of business on the second banking day following the settlement date of the original entry (i.e., one day to return an ACH debit).
- **Block all ACH debits except on a single account setup with an ACH debit filter or ACH Positive Pay.** 60% of AFP 2018 survey recipients implemented this practice. Anecdotally, customers using ACH Positive Pay report higher satisfaction and easier maintenance on their service than those with ACH debit filters.
- **Block ACH debits on all accounts** Otherwise known as an ACH Debit Block, this is a radical measure to preventing ACH fraud, but it does work for 35% of AFP 2018 survey recipients.

5 Effective Practices to Protect Against Wire Fraud

Recovering funds from fraudulent wire transfers is almost impossible; in many ways it is like sending cash to someone far away. Implementing effective practices is your best defense against wire fraud.

- **Stop and review before finalizing a wire.** Double check to make sure nothing seems amiss before releasing a wire. Unusual request methods, urgent or confidential labels are often used to discourage you from verifying the legitimacy of the request. Red flags should be explored in detail, not via email.
- **Annually review all established wire approval limits.** Employees may move to other positions over time, so it is important to establish routine checks to ensure that limits are still appropriately defined.
- ***Verify the authenticity of the request using an alternate method.*** If the request to initiate a wire came in via email, make a phone call to a known number to authenticate its legitimacy.
- **Implement dual control for initiating and releasing wire transfers.** Separation of duties, where one employee initiates the wire, and another approves it, is a common control used to not only protect against hackers but also to decrease the risk of internal errors.
- **Educate all employees involved in processing wire payments about payment fraud scams.** Regularly remind employees that Business Email Compromise (BEC) is the most common type of wire fraud with 77% of organizations surveyed reporting BEC attacks in 2017, according to the Association for Financial Professionals.

13 Ways to Protect Against Check Fraud

Commercial checks paid increased by 2% according to the Federal Reserve Payments Study (2017 Supplement) and account for 51% of all Business-to-Business (B2B) payments. This explains why check fraud remains the most targeted payment method by criminals. Some common best practices:

1. **Consider using alerts to notify you of checks presented for payment above a pre-specified dollar amount.** Even if you use positive pay, this can help keep your employees from creating a fraudulent check issue, if the alert goes to someone other than the employee who sends positive pay issue files.
2. **Secure *your check stock.*** In the event of a financial loss due to fraud, an argument can be made that the failure by a business to protect its check stock constitutes negligence. Routinely verify check stock to ensure preprinted checks (if you use them) remain in numerical sequence. A stolen check reorder notice has a street value of $100. Destroy checks using a cross-cut shredder under dual control.
3. ***Shred your paper trail.*** Any paper document containing sensitive information, even if they are old and relate to a closed account, should be securely discarded.
4. ***Enroll employees in direct deposit or use payroll cards whenever possible*** to eliminate or substantially reduce the number of paper checks.
5. ***Use warning bands on checks to deter perpetrators.*** Common warning bands include “check void after 180 days” or “account uses positive pay.” It is important to use warning bands in conjunction with a fraud notification service, such as stale date notification wherein the bank notifies you of any checks presented for payment beyond a designated number of days. Warning bands by themselves are not picked up by a bank’s equipment. If the check is deposited using an electronic service such as Remote Deposit, it may not be visually inspected by an individual before it is presented for payment against your account.
6. ***If you write more than 100 checks a month, use checks with high security features.*** For example, micro printing to create the border for 3-on-a-page checks and the signature line for laser checks which repeats the words "Original Document" cannot be duplicated by a typical copier or scanner. A color security pattern complicates attempts to alter the document using cut-and-paste forgery techniques.
7. ***Cause a check to expire before replacing it.*** Print an expiration statement on the check, such as “void 20 days from issue date,” and wait 20 + 2 days before reissuing it so that you are not held liable for both checks. Check cashing companies that accept an expired check have little basis to sue you using the “holder in due course” argument, if the check is returned.
8. ***Consider migrating check payments to single use purchasing card accounts.*** Single use cards, also called virtual cards, are considered the lowest risk of the various payment types because they use a 16-digit, virtual account for each payment. These cards also let you set the credit limit to the specific payment amount and the valid date range.
9. ***Use care when mailing checks.*** Always use security envelopes and do not leave them in a tray set beside a drop box or in a high-traffic area
10. ***Annual reports should not contain the actual signatures of executive officers.*** It is very easy to find these reports on the Internet, allowing perpetrators to reproduce signatures on checks, purchase orders, letters of credit, etc.
11. ***Consider opening a separate account used exclusively for incoming credits***, such as ACH and wire transfers. Place the new account on “no check activity” status and make it a zero-balance account, so that it will automatically transfer funds to your main account while preventing fraudulent checks from paying on your account.
12. ***Do not sign checks when you are in a hurry***, as it is very easy to slip in checks undetected when you are not closely reviewing them. Consider limiting your check runs to published dates. Use purchasing cards for emergencies.
13. ***Mail checks directly to the vendor once they are signed*** and do not send them back through the processing chain.

Best Practices for Your Company

4 Things You Should Train Your Employees to Do

Over three-fourths of finance professionals report that they have implemented education and training programs to help staff recognize potential payments fraud. Some ideas to consider:

- **Test your employees' knowledge of how to respond to spear phishing/clickbait attacks.** The 2017 Treasury Fraud and Controls Survey by the Strategic Treasurer reported that 27% of companies surveyed send fake phishing emails to employees to ensure they are properly trained in how to respond to attacks. The companies report that this has significantly reduced the success rate of BEC (business email compromise) attacks on their company.
- **Train employees to recognize social engineering tactics used to gain illicit information:**
  - Creating a sense of urgency. When fraudsters create an emergency situation, the victim may be more willing to accommodate their requests for illicit information.
  - Claiming a position of authority. A low-level employee is more likely to accommodate a request for sensitive information if it comes from a person with authority in the company.
  - Requesting sensitive information. A common technique is to call several different sources in an area and gather small bits of information from each person. The attacker can then piece this information together to gain further access.
  - Impersonating a fellow employee. Claiming to be from another internal department, the attacker may provide some general information and then ask for additional details
- **Ensure all employees are aware of "red flags" that signal their computer or Internet session may have been compromised**. Common red flags include:
  - Inability to log into an online banking site, despite multiple attempts with known password. This is an indication that the password and/or security questions have been compromised, or that the user ID is already logged in from another computer.
  - Sign on session to a website looks different than usual, possibly requesting additional information that is not normally required such as token information, answers to security questions, etc.
  - Redirection to an unsecured http website (instead of https://), particularly if there are spelling or grammatical errors on the website.
  - Pop-up window opens on the website, requesting personal information, account information, passwords, etc.
- **Mask account numbers and social security numbers whenever possible.** Delete the middle 8 digits of any social security numbers in the system. Do not forget to mask these same numbers in emails!

8 Action Steps to Protect Against Employee Fraud

While the vast majority (65%) of payment fraud occurs from external individuals according to AFP's 2018 study, external fraud attacks cost companies no more than half a percent of the organization's total revenue. Conversely, internal fraud may only occur 35% of the time, but according to the Association of Certified Fraud Examiners (ACFE), a typical organization loses 5% percent of annual revenue to fraud committed by people inside the organization. Internal fraud acts run an average of 18 months. Ways in which to manage internal risks include:

- Require employees to take consecutive vacation days.
- Assign dual system administrators for online cash management services.
- Perform routine and surprise spot checks.
- Do background checks on employees in financial or mail room positions.
- Be alert for behavioral red flags.
- Review invoices that may not be congruent with the nature of your business.
- Avoid invoice copies.
- Disable a terminated employee's computer access (including user IDs) and voicemail, as part of the exist procedure.

5 Examples of Business Email Compromise (BEC) Attacks

A BEC is a form of phishing attack where a cyber-criminal impersonates an executive and attempts to get an authorized employee to transfer funds or sensitive information to the criminal. These are highly focused attacks where cyber criminals will research employees and study news to make it seem as legitimate as possible.

- **Executive fraud** – the criminal hacked or spoofed an executive's email account then sends an email to an employee with wire transfer authority to send funds to an account owned by the cyber-criminal.
- **Bogus invoice** - the criminal has compromised an executive's email account, looks for an invoice or bill that is due soon and then contacts finance with revised payment instructions.
- **Attorney impersonation** – the criminal will impersonate a company's law firm and request funds to settle a legal dispute. In many cases the criminal will inject a sense of confidentiality and urgency to the request to discourage employees from verifying it.
- **Account compromise** – the criminal will hack an employee's email account to send customers an alert that there was a problem with their payment and they need to resend it to a different account, one owned by the criminal.
- **Data theft** – the criminal has compromised an executive's email account and asks HR or finance to send sensitive information to them. This is typically a precursor to a larger and more damaging cyber-attack.

4 Things to Include in a Data Breach Response Plan

Every company should have a data breach response plan. It is not a question IF your network will be breached, the only question is WHEN. While every plan will be unique to the company, there are 4 key elements that every plan must have.

- ***The type of data that constitutes a data incident*** – while this can vary substantially, in general it is defined as breaches that involve legally protected information and/or that represent a material loss to the company.
- ***The parties responsible during a data breach*** – defining roles and responsibilities is a critical element to detail and typically includes representatives from IT Security, Legal, Communications, HR and Executives.
- ***The internal escalation process*** – you need a well-defined process for escalating the incident up through your organization. Remove as much ambiguity as possible to remove the potential for embarrassing errors and costly mistakes.
- ***The external escalation process*** – your plan needs to designate precisely when outside help should be considered and what type of help to include. This can include forensic investigation teams or a 'breach coach' to help coordinate responses and customer notifications, determine legal obligations, and more.

4 Ways to Protect Against Ransomware Attacks

Verizon's 2017 Data Breach Investigations Report noted that ransomware went from the 22nd most common form of malware in 2014 to the fifth in 2016. Four good habits to start so you can protect your company from ransomware attacks include:

- Always download the latest version of software when it is available and run the updates.
- Back up files on an external hard drive that is not connected to the internet, if possible. This is hard to do but the thought is that this would mean you do not lose any information if you are hit by a ransomware attack.
- Never open a suspicious email attachment or download an app that you haven't verified with the store or merchant. In many cases it is a good idea to read reviews before installing mobile apps.
- Use antivirus programs to scan files before you download them. The ability to detect ransomware is built-in to most antivirus programs.

Common Scams and Schemes

4 Types of Bitcoin Scams

According to Zerofox, a digital risk monitoring company, there is a dark side to bitcoin. Here are some ways to spot scams:

- **Malware downloads.** Users are encouraged to click through fake bitcoin surveys that lures the user to download a malware-laden app. Use caution when looking at a social media URL that is shortened or not secured with an HTTPS connection.
- **Bitcoin phishing impersonators.** A website will offer a search service to entice users to enter their private bitcoin key to see if it exists in the database. Once entered, the scammer can spend directly from the bitcoin owner's wallet.
- **Bitcoin flipping scams.** Offer to instantly exchange bitcoins for money after paying an initial startup fee or a promise to double your investment overnight. The exchange is never made, and the bitcoins are immediately stolen.
- **Bitcoin pyramid schemes.** Similar to a traditional pyramid scheme, scammers promise that a low initial investment will be multiplied by signing up additional members using referral links. At some point the scammer walks away and the pyramid collapses.

5 Types of Social Media Attacks

Assume that social media threats are a business issue and familiarize yourself with the most common social media attacks:

- ***Fake Offering.*** These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.
- ***Manual Sharing Scams.*** These rely on victims to actually do the hard work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.
- ***Likejacking.*** Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.
- ***Comment Jacking.*** Similar to Likejacking, this type of scam relies on users clicking links that are added to comments by attackers. The links may lead to malware or survey scams.
- ***Fake Apps.*** Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data.

5 Things to Do If You Are the Victim of a Phishing Scheme

Phishing schemes are scams wherein cybercriminals try to trick you into sharing your sensitive data. Due to the variety of phishing schemes, what you'll do next depends on what kind of phisher targeted you.

- ***Focus on the details.*** *Try* to remember exactly what information you entered on the fraudulent website. Take screenshots of the phishing email or jot down details such as the sender's email address, the content of the email and the URL that you clicked.
- ***Change your password.*** If you clicked a link that directed you to a site that appeared to be your bank, email service or other key site, log into the real site (not using the link) and change your password. Take the extra time to change any password hints or security questions.
- ***Contact the organization that was spoofed.*** You may need to cancel cards and open new accounts.
- ***Watch out for warning signs of identity theft.*** Keep a close eye on your bank and card statements, looking for any withdrawals or purchases you did not authorize.
- ***File a report with the Federal Trade Commission (FTC)*** if you see signs that your identity has been stolen. The FTC will guide you through steps to take.

3 New Payment Fraud Schemes

Every day criminals come up with new ways to try to defraud your company. Some of the newer schemes include:

- **Card Testing**

Fraudsters can purchase lists of credit card numbers online on the "Dark Web" at a low cost but often do not know if the cards they are purchasing are active. To test these cards, fraudsters often use automated bots and scripts to run many of these numbers through a merchant's checkout page. Card testing fraud can be extremely costly due to financial charges (chargeback and processing fees) and loss of goods. Chargeback disputes typically take 6 weeks to materialize. Here are a few common red flags (used in combination with each other) to look out for:

- Small value transactions – Card testers typically use small value transactions to minimize the amount of credit card balance used.
- Multiple credit card purchases in a short amount of time – Fraudsters often use automated programs to run many cards through a website in a short time frame.
- Multiple credit card types – Credit card brands switching rapidly could be a signal of card testing fraud.
- Failed authorization notices – Multiple transaction failures may point to attempts to enter stolen card data.
- Address Verification Service (AVS) mismatch – Identifying that the address provided by the customer matches the billing address can provide an extra layer of protection. A mismatch can indicate a fraudulent transaction in which the customer is not the actual cardholder.
- Card Verification Value (CVV) mismatch – Validating the Card Verification Value (a security code typically printed on the back of the card) can verify that the customer is the cardholder and is in possession of the physical card. CVV mismatches should be monitored carefully.

Overpayment Fraud

Payout scams are no longer limited to conning people to sending money for fake job offers or get-rich-quick schemes. A common scheme is a fraudster presenting themselves as requiring the use of a preferred freight company to ship goods overseas. Using a stolen card, the fraudster pays the business for the goods and fake freight fee, often including a gratuity for the seller as an incentive to go along with the payout plan.

The business complies and pays the fee to the fake freight company, but no shipment ever occurs because it is not a legitimate shipper. The true cardholder discovers the unauthorized charge and disputes it. The business is then forced to reimburse in full, along with an additional penalty fee, even though they have paid out these funds to a fraudulent third party.

Transaction Laundering

Transaction laundering is a digital version of money laundering where cyber criminals use legitimate payment processes to sell illicit goods and services online. It is critical to know your customers very well and to research questionable behavior. It is common for site owners engaged in this to have two sites, one engaged in selling legitimate items and another one selling illegal goods or services. Both sites will use the same payment processing engine. The risk to the payment processor is that as far as the government is concerned, the payment processor is responsible and held financially or even criminally liable, regardless of whether or not the processor had knowledge of the illicit activities.