White paper

Establishing payments fraud policy and procedure

Payments fraud is on the rise. Annual surveys conducted by the Association for Financial Professionals (AFP) indicate that payments fraud activity has been steadily climbing since 2013. In fact, it reached new heights in 2017, when 78% of companies reported being targeted.[1]

Fortunately, there's a strategy that enables organizations to fight back against this trend, minimize fraud losses and reputational damage, and impress business insurers: establishing written policy and procedure for mitigating payments fraud risk.

AN UPDATE ON PAYMENTS FRAUD RISK

Fraudsters are adept at attacking all methods of payment, both paper and electronic, so it's always important to keep your eye on trends as you look to shore up your organization's defenses.

With that in mind, according to the 2018 AFP Payments Fraud and Control Survey, checks continue to be subject to more payments fraud than any other payment method. In 2017, nearly three-quarters of organizations responding to the survey experienced check fraud, the AFP reports.

The majority of payments fraud activity originates from individuals outside of the company through forged checks, stolen cards, or business email compromise (BEC), according to the AFP's survey report.

In 2017, more than three-quarters of organizations responding to the survey experienced a BEC attack, which AFP credits with leading to a dramatic increase in wire transfer fraud (more than tripling the number of incidents in 2014). According to the FBI, BEC "is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."

Between October 2013 and May 2018, in the United States alone, there were more than 41,000 victims of BEC or its close kin, email account compromise, resulting in losses approaching $3 billion. Domestic and international exposed dollar losses from such scams combined to reach $12.5 billion during that period. Participants in real estate transactions have been popular targets, the FBI notes.[2]

(continued)

BANK SOLUTIONS TO COMPLEMENT YOUR POLICY AND PROCEDURE

Ask your financial institution about how these security tools and practices can complement your payments fraud policy and procedures:

- Dual administration
- Dual approval on all electronic payments
- Alert notifications
- Transaction limit thresholds
- User entitlements management and review
- IP address restriction
- Secure token authentication
- Payee Positive Pay/ACH Positive Pay
- Account Reconcilement and Information Reporting
- ACH Blocks
- Universal Payment ID

MUFG Union Bank, N.A.
A member of MUFG, a global financial group

MUFG

Employees are another potential source of payments fraud risk that needs to be addressed in policy and procedure. According to the Association of Certified Fraud Examiners (ACFE), internal control weaknesses were responsible for nearly half of all employee fraud incidents, and asset misappropriation schemes are the most common form of such fraud. Asset misappropriation includes a number of fraudulent disbursement scams, including billing, payroll and expense reimbursement schemes, as well as check and payment tampering. The median loss from such attacks is $114,000.[3]

FRAUD'S IMPACT

Smaller and medium-sized enterprises often take the biggest hits from payments fraud. Research conducted by the National Cyber Security Alliance found, for instance, that more than 70% of cyber attacks target small businesses and as much as 60% of hacked small and medium-sized enterprises go out of business after six months.[4]

However, even the largest corporations have much to fear from payments fraud. While its survey shows that fraud attacks cost the vast majority of respondents no more than half a percent of total revenue, the AFP notes that the risk of reputational damage from fraud can be far more significant than the risk of a direct financial loss.

THE RATIONALE FOR A PAYMENTS FRAUD POLICY

The fact that payments fraud is rampant and growing is the biggest reason why organizations need to develop payments fraud policy and procedures. Another compelling reason is the potentially devastating impact of these attacks.

The monetary loss or reputational damage from a payments fraud can send some companies into a tailspin. Having a policy and procedures in place to prevent such a disaster just makes good sense from a risk management perspective.

Written policies and procedures are a risk management best practice. Just think about the important role that investment policies play in ensuring companies avoid questionable investments that don't fall within the risk profiles of their owners or boards of directors. Payments fraud policies can play a similar protective role.

A payments fraud policy can also provide needed direction on how to mobilize a response if and when a fraud attack is uncovered.

What's more, insurers have started asking to see companies' payments fraud policies and procedures when those companies are applying for business insurance coverage.

COMPONENTS OF AN EFFECTIVE POLICY

A payments fraud policy can be standalone or incorporated as part of a comprehensive fraud policy. Every organization is different, so every policy needs to be customized. But here are some common elements to consider including in your organization's written payments fraud policy:

A DESCRIPTION OF PAYMENT FRAUD RISK EXPOSURES

Your policy should define your organization's payments fraud threat landscape. This requires a review of all payment methods (e.g., checks, Automated Clearing House (ACH) payments, wire transfer and cards) and identification of all related potential fraud risks and schemes. The specific risks your organization faces can be gleaned through industry research, interviews with employees, brainstorming sessions, and other methods.

For example, in connection with wire transfers, you might note specific fraud schemes such as system password compromise, forged authorizations, and unauthorized transfer accounts. Similarly, for check and credit card fraud, you might list counterfeiting checks, check theft, stop payment orders, unauthorized or lost credit cards, counterfeit credit cards, and mail theft.

A PAYMENTS FRAUD RISK EVALUATION FRAMEWORK

Consider developing a table within your policy that for each identified risk notes:

- Likelihood of occurrence (i.e., probable, reasonably possible, remote)
- Significance if it does occur (i.e., immaterial, significant, material)
- The people and/or department subject to the risk
- Existing anti-fraud internal controls
- Assessment of internal controls effectiveness. Do you have a process in place to evaluate whether the controls are operating effectively and mitigating fraud risks as intended?
- Residual risks. What fraud risks aren't being mitigated adequately?
- Residual risk response. This could be a combination of implementing additional controls and designing fraud auditing techniques, or it could be to exit the activity creating the risk.

Your policy can indicate how often this fraud risk assessment should be updated.

(continued)

ASSIGNMENT OF FRAUD CONTROL RESPONSIBILITIES

Who specifically is responsible for payments fraud control at your organization? Some companies assign one individual to act as the fraud control officer. Your policy should outline all of that person's specific responsibilities related to fraud risk assessment, awareness, detection, reporting, and investigations.

Another policy strategy is to construct a fraud responsibility matrix that specifies what units or titles are responsible for particular actions, such as fraud-prevention controls, incident reporting, fraud investigations, internal control reviews, etc.

PROCEDURES FOR REPORTING FRAUD.

Your policy can outline who the employee who discovers the fraud should contact (i.e., an investigations unit or the legal department) and any rules or expectations about maintaining that employee's anonymity. The policy could also note any directives the whistleblower should be given, such as not discussing the case with anyone else.

PROCEDURES FOR INVESTIGATING FRAUD INCIDENTS

The policy could outline which unit within the organization is responsible for investigating suspected fraudulent acts, and the type of access that unit will have to company records in the course of its investigation. The policy could also document who in the company that unit should report any substantiated fraudulent act to, and how decisions about reporting such acts to authorities should be made.

EMPLOYEE MANAGEMENT STRATEGIES AIMED AT REDUCING INTERNAL FRAUD RISK

Some strategies that might be included in your policy are pre-employment screening, annual vacation requirements, rotation of job responsibilities, and taking out fidelity guarantee and criminal conduct insurance to indemnify the employer against losses related to employee fraud.

IMPLEMENTING THE POLICY AND PROCEDURES

There are two keys to successfully implementing a payments fraud policy.

One is to make sure that top management plays a central role in both formally approving and introducing the policy to the rank and file. Any fraud policy initiative needs to have the explicit backing of top management to ensure employee compliance.

The second is employee education and training. From their first day, employees need to be made aware of payments fraud policy and procedures — and how to recognize common fraud scams — and that can only be accomplished through regular training sessions and testing.

Finally, it's wise to partner with your financial institution on the development of payments fraud policy and procedures. Banks have deep experience working with commercial clients to protect their assets and can offer a variety of payments fraud prevention and detection solutions.

[1] AFP Payments Fraud and Control Survey Report, April 2018 https://dynamic.afponline.org/paymentsfraud/p/1

[2] FBI Public Service Announcement, July 12, 2018 https://www.ic3.gov/media/2018/180712.aspx)

[3] *2018 Report to the Nations*, Association of Certified Fraud Examiners https://www.acfe.com/report-to-the-nations/2018/

[4] *60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think)*, by Thomas Koulopoulos, inc.com, May 11, 2017. https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html

8914425-M (10/18)