FRAUD PREVENTION FRIDAY

Friday, November 15, 2024

New Payee Name Validation Ability for Treasury Check Verification System

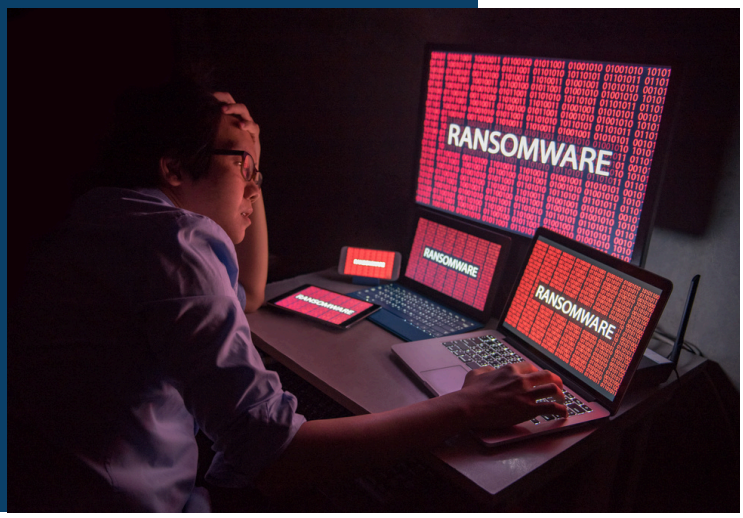
The Bureau of the Fiscal Service will implement a new payee name validation capability within the Treasury Check Verification System (TCVS) Application Programming Interface (API) on Nov. 18, 2024.

This new feature, mentioned in the Federal Reserve System's March 20, 2024, Notice to Financial Institutions, helps support Fiscal Service's payment integrity efforts by providing financial institutions with additional data to prevent check fraud.

- Payee name access will only be available through the API. The payee name cannot be accessed on the TCVS public website.
- Current API users can retrieve the new specification document on the TCVS website.
- To request a key for the API, complete the Terms & Conditions document (PDF) on the TCVS website.
- Service providers and financial institutions will not experience any impact on the current TCVS API process and can adapt to the new enhancement at their own pace after Nov. 18.

If you have any questions regarding this new enhancement, please send them to: paymentintegrity@fiscal.treasury.gov.

Top News



Gaining The Upper Hand on Ransomware

Size, complexity, and risk appetite are just words to ransomware threat actors. Here's how to gain an upper hand against ransomware threat actors.

Develop a crisis management plan.

Ransomware presents a unique challenge in that the time between detection and impact – the flash to bang – is essentially zero. Unlike cyber incidents that unfold over weeks, ransomware requires immediate execution of crisis management plans in real-time, without some of the normal phases of mitigation.

As you build the plan, identify the Incident Response (IR) team. It should include functions from across the organization, and all their actions should be driven by the Responsible, Accountable, Consulted, Informed (RACI) model.

Create a strategic response framework.

A solid response framework includes:

- Mission statement
- Strategies and goals
- Senior management approval (signed off/on)
- Organizational approach to incident response
- IR team's communication with the firm
- Metrics for incident response capability and effectiveness
- Roadmap for maturing the incident response capability
- IR program's role in overall organization

Test your plan throughout your organization to ensure it is ready to deploy in the event of an attack. With AI and other technological advancements, these threats will continue to increase. CBM members continue to be impacted by ransomware attacks.

Optimize Your Fraud Prevention Using a Layered Strategy

Did you know that data from the Federal Trade Commission shows **consumers reported losing nearly $9 billion to fraud in 2022, up 30% over the previous year?**

If your accountholders ask any search engine how to combat fraud, the response will likely include a list of tasks that can range from changing passwords frequently to tightening firewall configurations, and from using fraud monitoring software to freezing your credit report.

For your financial institution, however, combatting fraud is not that simple.

Adopt a Multi-Layered Fraud Prevention Strategy

In 2024, the name of the fraud prevention game is layers.

To fight back against fraud effectively, you need to adopt a robust, multi-layered defense strategy – one that provides layers of protection for your financial institution, staff, and accountholders, and also includes layers of transaction monitoring and solutions that provide you with meaningful and impactful alerts (and won't waste your time with a multitude of false positive events).

While some solutions are collaborative, bringing activity from various sources into one place for review, you may still need to review additional resources given the variety of fraudulent activities occurring over several communication and transaction channels.

(Click the link in the title to continue reading.)

Love At First Sight or Scam?

Many people turn to dating sites when looking for a new relationship. And while most individuals are genuine in their intentions, fraudsters flock to dating sites hoping unsuspecting users will swipe right on their fake profiles. Luckily, a reverse image search can help you investigate whether it's love at first sight or a scam.

What is a reverse image search?

Scammers often use fake photos to strike up a love connection to gain a person's affection and trust. The scammer uses the illusion of a romantic or close relationship as a way to steal money.

A reverse image search allows people to upload a photo on a dating site profile into a search engine, like Google, and check it against every photo across the internet. It will often reveal the true source of the image. It isn't a full-fledged guarantee it will reveal a scammer, but if your search results reveal multiple profiles using the same photo, it could be a sign your new crush could be a scammer.

Click here for detailed instructions on how to conduct a reverse image search on a computer and/or a mobile device.

Additional warning signs

The criminals who carry out romance scams are experts at what they do. They seem to be genuine and caring just to pull the rug out from under you once they get want they want. Protect your heart and your financial accounts with these additional ways to spot and avoid romance scams.

(Click the link in the title to continue reading.)

Your Smart Devices May Be an Invitation to Hackers

While you spend your time and energy guarding your community financial institution's (CFI's) central systems and technology against direct attacks by hackers, a back door into your systems may be vulnerable in ways you never imagined. Any device with an internet connection is potentially hackable. With the proliferation of smart devices, these back doors are multiplying.

The spread of smart devices has resulted in a host of new vulnerabilities. Often called the Internet of Things (IoT), these modern conveniences have been recognized as potential security problems. But those worries are often overlooked or downplayed. It's hard to imagine a fish tank as a security threat. There are actually quite a few seemingly harmless smart devices that pose a risk to your CFI if you haven't taken steps to secure them.

One of the top IoT device concerns at the moment is the office printer. Modern printers are far more advanced than earlier versions, offering myriad ways to print, scan, and copy, among other tasks. These multi-function printers are also typically connected to the internet, which can be a source of trouble: 61%of organizations dealt with data loss through their printers in 2023.

(Click the link in the title to continue reading.)