How U.S. Bank collects and safeguards your information

Since the events of September 11, 2001, banks and regulators are more focused on limiting the potential for financing terrorist and drug-related activities through our financial system. As a result, banks have increased their efforts to prevent money laundering and terrorist financing, and to comply with anti-money laundering (AML) regulations. These efforts are, in turn, a driving factor in determining which information is currently required from customers in order to process their transactions.

In August 2014, the U.S. government issued an Advanced Notice of Proposed Rulemaking entitled “Customer Due Diligence Requirements for Financial Institutions.” When final, the rule will require banks to verify the identities of “beneficial owners” of most legal entity customers, including corporations, LLCs, partnerships, unincorporated non-profits and statutory trusts. “Beneficial owner” is defined as “the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted.” Beneficial owner also pertains to an individual with an ultimate ownership stake of 25% or more of the equity interest, and an individual who exercises significant authority to control the legal entity customer’s affairs.

As a result of the enhanced due diligence requirements, U.S. Bank may request the following information and documentation from beneficial owners and authorized signers of new and existing legal entity customers:

- Full legal name
- Date of birth
- Current residential address
- Social Security number or other government-issued ID number for non-U.S. citizens

U.S. Bank, in some instances, may also request documentary evidence (e.g., driver’s license) to verify the information provided.

continued...
Information collected from beneficial owners or authorized signers is not shared outside of U.S. Bank, its subsidiaries or affiliates. Sharing this data within the bank only occurs for purposes of complying with anti-money laundering laws and regulations. Access to collected information is limited to users on a need-to-know basis.

U.S. Bank ranked first in the Ponemon Institute 2015 “Privacy Trust Study for Retail Banking” and has ranked first for the past nine years. We have a legal and ethical responsibility to ensure information is secure and accurately maintained.

U.S. Bank is committed to protecting the confidentiality, integrity, availability and privacy of our customers’ data. Our reputation rests, in part, upon securely maintaining our customers’ information assets.
Combatting destructive malware

Destructive malware continues to be a real, dynamic threat to businesses nationwide. It can compromise data and system confidentiality, availability and integrity. It can also disrupt business operations and harm brand reputation. Two high-profile cybersecurity incidents at large corporations help illustrate these negative effects. The first incident concerned an entertainment company that paid an estimated $8 million in legal settlement fees to employees whose personal data was breached. The second incident required a company to spend $40 million in recovery costs. Neither of these examples considers the amount of lost potential revenue from reputation damage.

At U.S. Bank, we encourage our customers to be aware of the ever-evolving cybersecurity landscape and evaluate the risk to their businesses. The Financial Services-Information Sharing and Analysis Center recently held a working group with participation from U.S. Bank to explore the growing risk of destructive malware. Based on their findings, we recommend you incorporate the following best practices into your organization’s risk management strategy as a measure to prepare for and combat against a destructive malware attack:

**Business recovery**
Develop, test, and update a crisis response and business recovery plan. Designate response and recovery team members, and include more than just the technology team. Involve legal counsel, a communications team, corporate management and the board of directors. Plan how your response team will engage with regulators and law enforcement.

**Malware detection**
Early detection can help prevent long-term damage. Use a combination of risk, signature and behavior-based detection techniques, working from network baselines. If a destructive malware attack is detected, a quick response is crucial and should include both containment and forensic analysis.

**Bare metal rebuild**
In the event of a cataclysmic destructive malware attack, consider a bare metal rebuild (BMR) when recovering systems and bringing networks back online. A BMR differs from restoring a computer as it involves rebuilding the servers from scratch—eliminating some human error, retaining settings and configurations, and lifting the administrative burden. A BMR can back up to any earlier available points, effectively restoring machines that may have been infected for longer periods of time.

*continued*
continued...

Lessons learned
Once it’s safe to reconnect to the network, incorporate any lessons learned immediately at both the technical and policy levels. Share threat indicators with partners, and include as much information as possible.

Employee education
Educate personnel on how to spot and avoid phishing and social engineering techniques. Training should be ongoing and include reporting procedures.

Backup solutions
Emphasize backup solutions, particularly offline backups, to facilitate a quick data restoration and maintain integrity.

Limit administrative access
Most users do not need the ability to modify user accounts or install software on computers IT teams are trying to manage for them. Removing administrative access from standard users can dramatically reduce the impact malware is able to make.

IBM Trusteer Rapport

If you believe that computers used to process financial transactions have been infected with malware, contact your U.S. Bank representative to secure your accounts.
Five tips to help safeguard your organization

Business Email Compromise (BEC) scams targeting domestic and foreign businesses that regularly perform wire transfers continue to be the number one threat to our customers’ financial assets. Data from the FBI estimates the total loss of this global threat to be in excess of $1.2 billion.* Based on several recent high-profile incidents, that number is sure to increase, emphasizing the need for heightened awareness and vigilance in executing key internal controls.

To help shield your organization from fraud, there are various internal control enhancements and security practices to consider. While no single control or set of controls will offer absolute assurance, we suggest the following five tips:

1. **Confirm and verify email requests for fund transfers.** Contact the requestor by phone using an independently obtained phone number or one that you already have on file. Special scrutiny should be paid to transfers requested to new or recently updated accounts. Nearly all BEC scams can be stopped in their tracks if organizations adopt this basic control.

2. **Use dual control for money movement activities.** This allows for two levels of scrutiny and authorization to help stem the risk of illegitimate funds transfers.

3. **Use multi-factor authentication for web-based email accounts.** Fraudsters are known to leverage actual accounts of executives with email credentials pilfered from spear phishing campaigns. Multi-factor authentication adds another layer of control to deter cyber crooks from accessing employee accounts.

4. **Communicate quickly when fraud or security events occur.** Notify your key banking partners and information security staff immediately. If appropriate, contact law enforcement and file a complaint with the FBI’s Internet Crime Complaint Center.

5. **Create awareness within your organization.** Evaluate staff compliance with internal controls by using real-world security awareness testing.


Cybersecurity from an executive perspective

In preparation for the annual Executive Leadership Forum last fall, U.S. Bank administered a survey to determine the primary drivers of business decisions and risk oversight for executives. The survey was sent to forum registrants to provide forum speakers with a basis for their content; nearly 60 percent of the registrants participated in the survey. Focused on trending issues, opportunities and disruptions, responses to the survey emphasized the significance of cybersecurity in the current risk landscape and the importance of education on all lines of defense. Key cybersecurity results from the survey were:

**Threats**

Cybersecurity attacks on U.S. commercial and government networks, and the cybersecurity vulnerability of U.S. infrastructure and services ranked highest on the survey.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity attacks on U.S. commercial and government networks</td>
<td>71%</td>
</tr>
<tr>
<td>Cybersecurity vulnerabilities of U.S. infrastructure and services</td>
<td>56%</td>
</tr>
<tr>
<td>Domestic terrorism</td>
<td>42%</td>
</tr>
<tr>
<td>Russia's activism in Europe</td>
<td>40%</td>
</tr>
<tr>
<td>Renewed advances of nuclear weapons in countries such as Russia, China, Iran, and North Korea</td>
<td>36%</td>
</tr>
<tr>
<td>Pan-national terrorist organizations</td>
<td>27%</td>
</tr>
<tr>
<td>Large scale population movements due to political and civil unrest abroad</td>
<td>22%</td>
</tr>
<tr>
<td>High sovereign debt levels and weak economies in countries such as Greece</td>
<td>15%</td>
</tr>
<tr>
<td>China’s military ambitions</td>
<td>11%</td>
</tr>
<tr>
<td>Cross-border movements of weapons</td>
<td>5%</td>
</tr>
</tbody>
</table>

**Securenness**

Banking and financial systems, data networks and internal corporate networks were considered the most secure. Natural gas supply lines, electric power supplies and mobile communication networks were ranked lowest.

---

continued…
continued…

Awareness
Survey participants perceived that within their companies, top management and those responsible for oversight have a keen understanding of cybersecurity risks. Mid-level managers and front line personnel were perceived as considerably less aware.

Although the results of the survey are not unexpected, they reinforce the risks of doing business in a highly-connected and changing technology environment. The results stress the importance of protecting your organization, employees and customers. Here’s how this can be accomplished:

• Estimate current cyber security risks and trends on an ongoing basis and take adequate precautions against them.

• Maintain an employee awareness program on social engineering attacks prevention.

• Assess your organization’s current level of awareness at each business layer.

• Implement a social engineering campaign with additional training and/or conduct periodic assessments.

• Evaluate the efficacy of your current detection software and internal controls. Determine whether they are adequate to defend your organization against a cyber attack.